(19) Japanese Patent Office (JP)

(12) Publication of Unexamined Patent Application (A)

(11) Disclosure number
Unexamined patent 2002-217894 (P2002-217894A)
(43) Disclosure date: October 2, 2002

(51) Int.Cl.[7]	ID symbol	FI			Theme code (reference)
H04L 9/08		G06F	13/00	520B	5C052
G06F 13/00	520		17/60	302E	5C053
17/60	302			332	5C064
	332			ZEC	5J104
	ZEC	H04N	5/76	Z	

Request for examination not filed Number of claims: 17 OL (43 pages in all)

(21) Application number: Pat. Appl. 2001-295722 (P2001-295722)

(22) Filing date: September 27, 2001

(31) Priority declaration number: Pat. Appl. 2000-300566 (P2000-300566)

(32) Priority date: September 28, 2000

(33) Priority declaration country: Japan (JP)

(71) Applicant: 000005108
Hitachi Ltd.
4-6 Surugadai, Kanda, Chiyoda-ku, Tokyo

(72) Inventor: Hiromi Harada
in Broadcasting and Communication Systems
Promotion Sales Department, Hitachi Ltd.
4-6 Surugadai, Kanda, Chiyoda-ku, Tokyo

(72) Inventor: Kaoru Onishi
in Broadcasting and Communication Systems
Promotion Sales Department, Hitachi Ltd.
4-6 Surugadai, Kanda, Chiyoda-ku, Tokyo

(74) Agent: 100107010
Ken Hashizume, Patent Attorney

Continued on last page

(54) [Title of invention] Data distribution service method

(57) [Abstract]

[Problem] To provide content control service using the detailed information concerning content.

[Solution means] A service is provided that can protect copyright and other content rights by defining on the broadcasting side the method of presentation of content to viewers, conditions of use, content storage in encrypted form, restricted reception to terminals, restricted reception to individuals, etc., distributing the defined description, together with the content, to the reception side, and carrying out viewers' viewing control, storage control, computer control, encryption/decryption control, etc. To this end, a comprehensive data distribution system appends metadata, which is content-related information, to each item of content. This metadata gives general information such as the title, nature, and composition of the content, control information concerning storage and playback processing, control information concerning billing, and information concerning copyright protection, such as information concerning the content encryption method including content decryption keys, etc.

1 content

content

4 storage medium content

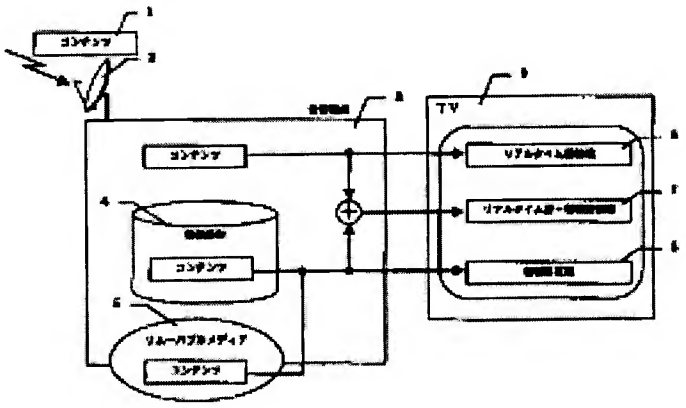
5 removable media content

3 reception terminal

6 real-time viewing

7 real-time + stored viewing

8 stored viewing



[Claims]

[Claim 1] In a data distribution service method in which content is distributed using media such as satellite, terrestrial circuits or other communication circuits, or removable media,

a data distribution service method in which

the transmission-side device

performs encryption of the content after generation of the content,

divides the encrypted content into blocks,

stores each element of the block-divided encrypted content in the payload part of the distribution stream, assembles them into a distribution data format, and distributes the content, and

generates and distributes metadata in which are stored the method of presentation of the content, its conditions of use, and content-related information including the encryption key of the content; and

the reception terminal,

if it assembles content, assembles the payload part without decryption, and stores content and metadata in still encrypted form, and

performs billing control and rights protection with respect to the content by making judgments concerning use of the content on the reception side.

[Claim 2] In the data distribution service method of claim 1, a data distribution service method in which

in the encryption of the content, encryption is performed on all the data in each element constituting the content, and

for the metadata, encryption is applied only to predetermined necessary parts.

[Claim 3] In a data distribution service method in which content is distributed using media such as satellite, terrestrial circuits or other communication circuits, or removable media,

a data distribution service method that includes

a step in which the reception terminal makes the transmission-side device a contract request that includes the terminal ID the user has contracted to a fee-charging business, the personal ID, and the channel or program or content he wants to contract,

a step in which the transmission-side device, according to the contract request that has been made, generates metadata for prior contract, leaves the terminal ID and personal ID unencrypted, encrypts, with a terminal key Kmc unique to each reception terminal, contract information that includes the fee-charging business ID, a business key Kw unique to each business, and the contract code, and distributes it to the reception terminals,

a step in which the reception terminal decides, according to the terminal ID and personal ID stored in the unencrypted part of the metadata for prior contract, whether it is information addressed to the user who is to use the terminal, and if it is decided that it is addressed to the using user, decrypts the metadata for prior contract by the terminal key Kmc that is prestored in the reception terminal, and obtains contract information including the business key Kw,

a step in which the reception terminal, based on the obtained contract information, makes a request for content to be broadcast by the contract business;

a step in which the transmission-side device causes synchronization with the distribution of the encrypted content, including keeping the fee-charging business ID unencrypted, distributes metadata for key distribution in which the necessary part, including the encryption key Kk of the content that will be needed when viewing the content, is encrypted with the business key Kw, and metadata for storage/playback in which the necessary part, including the use restrictions information for the content that includes the content distribution device position, is encrypted with the content [encryption] key Kk; and

a step in which the reception terminal causes synchronization with the encrypted content, receives metadata for key distribution that is distributed, decides by the fee-charging business ID that is stored in the unencrypted part whether it is a broadcast by the contract business, and if it is decided that it is metadata for key distribution to the content to be broadcast by the contracted business, decrypts the encrypted part by the business key Kw distributed by the metadata for prior contract, decides by the decrypted relevant contract code and the contract code distributed by the metadata for prior contract whether it is usable content within the user's contract form, and if it is usable, stores the content key Kk in the reception terminal, decrypts by the content key Kk the encrypted part of the metadata for storage/playback received at the same time, confirms the use restrictions information with respect to the content, and if it can be used by the user, receives the encrypted content according to the distribution location information of the encrypted content stored in the metadata for storage/playback.

[Claim 4] In a data distribution service method as described in claim 1 or 3, a data distribution service method that is characterized in that

in order to provide service to the user in various element units such as content units, channel units, program units, or file units in a computer, service can be provided in content units designated by the reception terminal, in which the transmitting-side device designates a unit indicating a physical quantity of the content, and distribution is done with the designated physical quantity included in the metadata.

[Claim 5] In a data distribution service method as described in claim 1 or 3, a data distribution service method that is characterized in that

the metadata includes information including the title and nature of the content, the method presentation of the content to the viewer defined on the transmission side, and the conditions of use;

the transmission-side device encrypts the necessary parts also with the metadata itself to prevent data tampering and maintain secrecy and then distributes it; and

the reception terminal stores the metadata in still encrypted form, and at the time of use ensures rights protection by controlling the reception terminal by the encryption key.

[Claim 6] In the data distribution service method of claim 1 or 3, a data distribution service method that is characterized in that

the metadata for prior contract is metadata that includes the business key Kw of the fee-charging business and contract code content concerning the form of the contract, and is distributed when a terminal is purchased, when a contract is updated, or when a business key Kw is updated;

the metadata for the EPG [electronic program guide] is metadata for confirmation of content that is scheduled to be distributed or for making a reservation;

the metadata for storage/playback is metadata that includes information needed for the reception, storage, and playback of content;

the metadata for key distribution is metadata that distributes information concerning encryption keys for content;

the metadata list is metadata for acquiring the distribution position of metadata items within the distribution stream;

the metadata for system key updating is metadata for updating the system key Ksy that is common to all reception terminals; and

the transmission-side device distributes the metadata classified, according to its purpose of use on the reception terminal side, its distribution timing on the transmission side, and its description, into metadata for prior contract, metadata for the EPG [electronic program guide], metadata for storage/playback, metadata for key distribution, metadata for system key updating, and the metadata list.

[Claim 7] In a data distribution service method as described in claim 6, a system that is characterized in that

what is in the metadata for prior contract that is distributed to users individually is individual users' contract information; what is stored in the key distribution metadata and storage/playback for the various content that is distributed in common to all users are the contract information and conditions of use, etc. that will be necessary; a comparison is made between the individual users' contract information that is distributed by the metadata for prior contract and the contract information included in the other metadata, use of the content by the user is made, and restricted reception in content units to individual users is carried out.

[Claim 8] In a data distribution service method as described in claim 6, a data distribution service method that is characterized in that

information for which rights protection is necessary, including contract information for each user and the business key Kw for each business, is stored in the metadata for prior contract, and the transmission-side device, by encrypting this information by the terminal key Kmc of each terminal owned by each user or by a personal key Km, distributes the information while safeguarding the secrecy of the information.

[Claim 9] In a data distribution service method as described in claim 6, a data distribution service method that is characterized in that

the metadata for the EPG [electronic program guide] is for confirmation of content that is scheduled to be distributed or for making a reservation, and in it is stored information for which rights protection is necessary, including use restrictions information; and

the transmission-side device, by encrypting this information by the common key Ksy for all reception terminals, distributes it to all users without distinction among users, while maintaining the secrecy of the necessary information in the metadata.

[Claim 10] In a data distribution service method as described in claim 6, a data distribution service method that is characterized in that

content rights protection is realized by making it so that for metadata for key distribution in which information is stored including encryption keys for content and for metadata for storage and playback in which information is stored including content copy control information, by the transmission-side device distributing the metadata for key distribution encrypted by the business key Kw and the metadata for storage and playback encrypted by the content key Kk for each content, only users who have made a contract with the business and have received the business key by the metadata for prior contract will be able to acquire the content key Kk.

[Claim 11] In a data distribution service method as described in claim 6,

the metadata for key distribution distributes information concerning the encryption key for content; and

if the content is a for-fee broadcast, the transmission-side device encrypts the information by the business key Kw unique to each business, and if the metadata corresponds to free content that can be viewed even by users other than contracting parties, it encrypts it by the system key Ksy that is common to all reception terminals.

[Claim 12] In a data distribution service method as described in claim 6, a data distribution service method that is characterized in that

the metadata for system key updating is metadata in which is stored information for updating the information that is common to the system as a whole, including the system key that is common to all the reception terminals within the system; and

the transmission-side device, by encrypting the part for which protection is necessary, including the new system key Ksy3, using the spare system key Ksy2 that is kept ready in advance in common among all the reception terminals, is able to distribute it without distinction among users while maintaining the secrecy of the necessary part within the metadata.

[Claim 13] In a data distribution service method as described in claim 6, a data distribution service method that is characterized in that

the metadata list stores the distribution position along the distribution channel of each metadata list being distributed, and the reception terminal acquires metadata using the metadata list.

[Claim 14] In a data distribution service method as described in claim 6, a data distribution service method as described that is characterized in that

by storing in the metadata list information for recognizing updates of metadata for the EPG [electronic program guide], metadata for storage and playback, etc., it is possible to receive just the updated metadata.

[Claim 15] In the data distribution service method of claim 1 or 3,

encrypted metadata is distributed either if embedded distribution is done again in metadata that is not encrypted, or if it is distributed as a separate file.

[Claim 16] In the data distribution service method of claim 1 or 3, a data distribution service method that is characterized in that

the transmission-side device generates and manages customer information based on information including the terminal ID under which a user has purchased a reception terminal, the personal ID, the business one wants to contract with, and the number of points for using content, stores the number of points that are consented to in metadata for prior

contract, and distributes it to the reception terminals of contract users; and

the transmission-side device causes synchronization when distributing content, and stores and distributes information on the points required when using content in the metadata for storage/playback that is distributed; the reception terminal, when using the content, plays back the content and reduces the number of necessary points stored in the metadata for storage/playback by the number of points distributed by the metadata for prior contract; thereby one views content in the range of points distributed with the metadata for prior contract.

[Claim 17] In the data distribution service method of claim 1 or 3, a data distribution service method that is characterized in that

the transmission-side device generates and manages customer information based on information including the terminal ID under which a user has purchased a reception terminal, the personal ID, the business one wants to contract with, and the number of points for using content, stores in the metadata for prior contract, as online pay-per-view consent, information on the transmission destination at the time of billing information transmission, and distributes it to the reception terminals of contract users; the transmission-side device causes synchronization when distributing content, and stores, in the metadata for storage/playback that is distributed, information based on generating billing information when content is used; and the reception terminal to which it is distributed, when using the content, adds information including the ID of the using user to the information that serves as the basis for generating the billing information stored in the metadata for storage/playback, and using a terrestrial circuit transmits it to transmission destinations designated by the metadata for prior contract.

[Detailed Description of the Invention]

[0001]

[Field of technology to which the invention belongs] This invention relates to a data distribution service method in which content is provided on the content-providing side and is received and used on the using side; in particular, it concerns a data distribution service method that has an arrangement to protect content and has an arrangement to add metadata, which is content-related information, to the content and distribute it.

[0002]

[Prior art] Heretofore, broadcasting or communication using satellite waves or terrestrial waves has generally been real-time broadcasting, and in part stored-type communication has existed. With stored-type broadcasting or communication, it is possible to store the distributed programs and information on a large-capacity storage medium by storage operations by the user himself. This allows the user to watch a program whenever he wants.

[0003] The usual way to protect the content of a real-time broadcast is to encrypt the content. Encryption makes illicit viewing and tampering difficult. One content encryption method is CAS (Conditional Access System), which is a method for restricted reception of BS [broadcast satellite] digital broadcasts. With CAS, the content is encrypted by a first encryption method, and the first decryption key for decrypting the encrypted content is encrypted by a second encryption method. Then the encrypted content and the first key are distributed to users. A user who can receive the content previously holds the second decryption key, which is the decryption key for the second encryption method. Thus only users who hold the second decryption key can receive the first encryption key, and only users who have been able to receive the first encryption key are able to receive the content. By using CAS in this way, only restricted users are able to obtain and watch content, and the users who are able to watch can be controlled. In BS digital broadcasting, SI (service information) is defined as information concerning content.

[0004]

[Problems that the invention is to solve] The prior-art CAS referred to above is a restricted reception method used in real-time broadcasting. With this method, decryption of the content takes place simultaneously with reception of the content. In doing so, reception control with respect to users is possible, but because the content gets decrypted, playback control is not possible. And when stored, the content is kept in plaintext form, so the content cannot be protected.

[0005] And in the current standards for satellite digital broadcasting, only SI [service information] exists as a means for defining information concerning content. This SI is content-related information, but because it is information for the EPG (electronic program guide), it is not described in detail. The broadcasting standards make no provisions for a means to define detailed information concerning various content, and this makes it impossible to offer finely worked-out service based on content-by-content control. Because of this, it is impossible to provide content control service using detailed information concerning content. And because broadcasting as it exists today assumes that content will be viewed in real time, information for content storage control and copy control is sparse, and is inadequate for use in stored-type broadcasting.

[0006] In view of the above points, the purpose of this invention is to provide a data distribution service method that adds control information that makes it possible to protect stored-type broadcasting and content.

[0007]

[Means of solving the problems] The comprehensive data distribution system of this invention provides an encryption method in which content is received in encrypted form, then is stored on a storage medium, and is decrypted for the first time upon playback of the content. Also, it appends metadata, which is content-related information for each content. Described in this metadata are, for example, general information such as the title, nature, and internal composition of the content, control information concerning storage and playback processing, control information concerning billing, and information concerning copyright protection, such as the content decryption key and other information concerning the content encryption method. Viewer viewing control, storage control, copy control, and encryption/decryption control are carried out based on this information. This makes it possible to have content rights protection and user rights protection.

[0008] According to the first solution means of this invention, in a data distribution service method in which content is distributed using media such as satellite, terrestrial circuits or other communication circuits, or removable media, a data distribution service method is provided in which the transmission-side device performs encryption of the content

after generation of the content, divides the encrypted content into blocks, stores each element of the block-divided encrypted content in the payload part of the distribution stream, assembles them into a distribution data format, and distributes the content, and generates and distributes metadata in which are stored the method of presentation of the content, its conditions of use, and content-related information including the encryption key of the content; and the reception terminal, if it assembles content, assembles the payload part without decryption, and stores the content and metadata in still encrypted form, and performs billing control and rights protection with respect to the content by making judgments concerning use of the content on the reception side.

[0009] According to the second solution means of this invention, in a data distribution service method in which content is distributed using media such as satellite, terrestrial circuits or other communication circuits, or removable media, a data distribution service method is provided that includes a step in which the reception terminal makes to the transmission-side device a contract request that includes the terminal ID the user has contracted to a fee-charging business, the personal ID, and the channel or program or content he wants to contract; a step in which the transmission-side device, according to the contract request that has been made, generates metadata for prior contract, leaves the terminal ID and personal ID unencrypted, encrypts, with a terminal key Kmc unique to each reception terminal, contract information that includes the fee-charging business ID, a business key Kw unique to each business, and the contract code, and distributes it to the reception terminals; a step in which the reception terminal decides, according to the terminal ID and personal ID stored in the unencrypted part of the metadata for prior contract, whether it is information addressed to the user who is to use the terminal, and if it is decided that it is addressed to the using user, decrypts the metadata for prior contract by the terminal key Kmc that is prestored in the reception terminal, and obtains contract information including the business key Kw; a step in which the reception terminal, based on the obtained contract information, makes a request for content to be broadcast by the contract business; a step in which the transmission-side device causes synchronization with the distribution of the encrypted content, including keeping the fee-charging business ID unencrypted, distributes metadata for key distribution in which the necessary part, including the encryption key Kk of the content that will be needed when viewing the content, is encrypted with the business key Kw, and metadata for storage/playback in which the necessary part, including use restrictions information for the content that includes the content distribution device position, is encrypted with the content [encryption] key Kk; and a step in which the reception terminal causes synchronization with the encrypted content, receives metadata for key distribution that is distributed, decides by the fee-charging business ID that is stored in the unencrypted part whether it is a broadcast by the contract business, and if it is decided that it is metadata for key distribution to the content to be broadcast by the contracted business, decrypts the encrypted part by the business key Kw distributed by the metadata for prior contract, decides by the decrypted relevant contract code and the contract code distributed by the metadata for prior contract whether it is usable content within the user's contract form, and if it is usable, stores the content key Kk in the reception terminal, decrypts by the content key Kk the encrypted part of the metadata for storage/playback received at the same time, confirms the use restrictions information with respect to the content, and if it can be used by the user, receives the encrypted content according to the distribution location information of the encrypted content stored in the metadata for storage/playback.

[0010]

[Embodiments of the invention] 1. Overview

(Service overview) This "comprehensive data distribution service" is information (data) distribution service in which the content that one wants to see can be seen when and where one wants to see it; unlike conventional real-time (viewing what is being broadcast) digital broadcasting, stored-type information distribution is also done, with no limitation to the real-time type. Thus a service like Near Video On Demand (NVOD) is provided by which the viewer can select and watch preferred content from among stored content whenever he wants. It also offers content viewing wherever the user wants it by directly storing or copying content on removable media or on external equipment connected to a reception terminal that receives this service. In addition, while in conventional digital broadcasting service it is only a form of content use contract in a narrow range, such as a terminal-by-terminal contract, this service provides a form of content use contract in a wide range including contracts in units of individual users.

[0011] Figure 1 is a block diagram of the reception side of the comprehensive data distribution service. As an overview of this comprehensive data distribution service, we describe stored-type television broadcasting using Figure 1. On the reception side, it has an antenna 2, a reception terminal 3, and a television 9. "Stored-type television broadcasting" means an information distribution service in which content 1 (a program) sent from the broadcasting side (broadcasting station) like a conventional television broadcast is received by the antenna 2 (there are also the cases of distribution by cable and distribution by package) and receiver 3, and viewing takes place from the moment it is distributed on a television 9 or other monitor device; here, in addition to the case known as real-time viewing 6, services are available such as stored-type viewing 8 (sometimes a DVD-RAM or other removable media 5 abounding in transportability is used as the storage medium), in which content that has once been distributed is viewed after having been stored on a storage medium 4 (a hard disk or other large-capacity storage medium) as with a conventional video deck, and real-time + stored-type viewing 7, in which stored content and real-time content that is being distributed are combined and viewed.

[0012] (System overview) Figure 2 is a block diagram of the overall system for comprehensive data distribution service. As the system by which comprehensive data distribution service is carried out, besides infrastructure with electromagnetic waves such as satellite broadcasting or terrestrial broadcasting, service is possible with infrastructure that uses communication lines, such as cable television or the Internet, but with this invention, as an example, we describe the case in which the infrastructure is digital satellite broadcasting using a satellite as in Figure 2.

[0013] Using Figure 2, we give an overview of a system in which comprehensive data distribution service is provided. This comprehensive data distribution service system has a transmission side 100, a reception side 200, and a satellite [digital] circuit 10, terrestrial circuit 11, physical distribution network 12, and portable telephone network 13 that use a satellite that is a transmission channel that links the transmission side 100 and the reception side 200. The reception side 200, as the term is used here, is not necessarily just the reception terminal 3 that is installed in the home 201; it also assumes public terminals 202 such as vending machines, terminals installed at shops 203 such as convenience stores, on-board terminals 204 in moving vehicles such as automobiles, and portable terminals 205, etc. On the transmission side 100, it has a distribution center that produces and manages the content 1 and control information, etc. and distributes them to the reception side 200, a key management center that generates and manages keys to be used for content encryption, etc., a customer management center that manages reception-side user information, a terrestrial circuit management center that manages communication using terrestrial circuit 11 and portable telephones 206 for collecting requests and viewing histories, etc. from reception-side users, and a physical distribution management center that distributes (delivers) content to users and sales outlets, etc. by DVD and other package media.

[0014] (Nature of the services) Next we describe the services offered in the system of Figure 2. As services in this comprehensive data distribution service, there is, for example, first, service to the home 300, in which comprehensive data with videos, music, electronic magazines, games and other images, voice, and data is distributed to reception terminals 3 as digital information, using mainly a satellite digital circuit 10 as stated above. Second, there is service to vending machines/sale outlets 301, in which, as with service to the home 300, data is distributed to vending machines 202 and sales outlets 203; this handles data that is too voluminous to be stored in the home, the backup of data that is not stored, and data that can be sold only be vending machines and sales outlets; for example an electronic magazine that can be bought only at a sales outlet is purchased and viewed on a home reception terminal 3. Third, there is service to mobile bodies 302, in which content from a reception terminal 3 in the home or from a vending machine 202 or sales outlet 203 is carried to an external device such as an on-board device 204 or a portable terminal 205 and can be viewed outside the home; for example, map data distributed to a reception terminal in the home can be carried out to on-board equipment 204 using removable media like DVD or memory card ["IC" (integrated circuit) card in Japanese] and can be used inside the car, or music data can be carried out using a memory card or other removable media or a memory card and can be played on a portable terminal 205. Fourth, there is package delivery service 303, in which content that cannot be distributed by satellite circuit 10 is distributed by CD-ROM, DVD-ROM, or other package media using a physical distribution network 12; for example, if one reserves content such as a drama by a reception terminal, the content is delivered from the transmission side to the home on DVD-ROM, etc. by a home delivery service, etc. Fifth, there is service to portable telephones 304, in which a portable telephone 206 or other external equipment having a communication means is used, and by controlling a reception terminal in the home via the transmission side, program reservations, etc. are made to a home reception terminal from outdoors by, for example, an EPG (electronic program guide) on the screen of the portable telephone 206. In addition, the services are not limited to these; a wide range of services will be possible as the communication infrastructure is built up. In this embodiment, the explanation has focused on service to the home 300, but it can be applied to other services as well.

[0015] (Rights protection method) This comprehensive data distribution service is a service whose purpose is to distribute content directly to the home, etc. and store/copy/play it with digital data in the home, etc., and because this entails problems concerning rights such as copyrights involving data tampering and copying and playing that goes beyond personal use, it is necessary to protect and manage content copyrights and the rights of broadcasting businesses and viewers.

[0016] Figure 3 is an explanatory diagram of the rights protection method in a comprehensive data distribution service. Using Figure 3, we describe the rights protection method in this comprehensive data distribution service. The rights protection method in a comprehensive data distribution service is a method whereby, on the transmission side, metadata 18 in which is stored information including the method of presentation of content to viewers defined with respect to the content, the conditions of use, and the content encryption key is distributed along with the encrypted content (encryption content) 17 and other PSI/SI (Program Specific Information/Service Information), etc. 19, and on the other hand the metadata 18 is interpreted by the rights protection function 16 (RMP [Rights Management and Protection] function) on the side of the reception terminal 3, and control is carried out including reception control of the content 17 to the reception terminal 3, storage control with respect to storage medium 4 and removable media 5, copy control, encryption/decryption control, control of presentation to monitor devices such as TV 9, authentication control with respect to external equipment 14, and authentication/billing control with respect to memory cards 15 for identifying individuals.

[0017] Next, we describe the PSI/SI 19, content 17, and metadata 18 that is distributed by the transmission side. PSI/SI 19 means data for acquiring the needed data from the stream during distribution, as with conventional digital broadcasting; in this comprehensive data distribution service, it is used for acquiring metadata, encrypted content, etc. The distinction of the service from conventional digital broadcasting is made by the use of a service list descriptor stored in the NIT (Network Information Table) in the PSI, and a stream identification descriptor stored in the PMT (Program Map Table).

[0018] In this comprehensive data distribution service, content 17 is basically stored in still encrypted form in the storage medium 4 and removable media 5, etc., in order to prevent tampering and illicit use of the data. Also, the content 17 in the comprehensive data distribution service is conceptual; it is not a unit denoting a certain physical quantity but can be specified by any unit the transmission side intends, and the reception terminal can recognize the content by stating the designated physical quantity in the

metadata. Content is divided into image content, by moving pictures that can be viewed if one specifies a channel as with conventional digital broadcasting, and data content, which is focused mainly on viewing after it has been recorded.

[0019] Figure 50 is an example of an explanatory diagram of the data that constitutes image and data content. In this comprehensive data distribution service, each item of a set of data that constitutes content is called an element. Thus content is made up of one or more elements. In this comprehensive data distribution service, metadata 18 includes, for example, the content that is given to content that is designated in units intended by the broadcaster, which is the transmission side, general information used for retrieval, etc. of composition, etc., and the method of presentation to viewers and conditions of use of content whereby the protection of copyright holders and related rights is defined on the transmission side. Metadata can control terminals and protect rights according to all this information. Accordingly, because information to be protected is included, like content, in metadata, some of it is distributed encrypted, and when it is stored it is stored in still encrypted form. According to the distribution timing and its nature, metadata is classified into metadata for prior contract, metadata for the EPG [electronic program guide], metadata for storage/playback, and metadata for key distribution.

[0020] In metadata for prior contract are stored business keys, which are keys unique to each fee-charging business, and contract codes, etc. for interpreting on the reception terminal side whether all or part of a program broadcast by a contracted business can be viewed, etc., and distribution of content to an individual user is distributed asynchronously. In metadata for the EPG [electronic program guide] information is stored on reception terminal side such as confirmation of the content to be distributed, and the title, nature, scheduled broadcast date, and other information required for making a viewing/storing reservation; before distribution of content without distinction of users who use a reception terminal, it is distributed to all reception terminals; it is mainly for EPG [electronic program guide] display on reception terminals and for making reservations to schedule viewing/storage. In metadata for storage/playback, information is stored for receiving and storing content and for carrying out viewing contracts with respect to content; it is distributed simultaneously with the distribution of content for all reception terminals, without distinction of users who use reception terminals. In metadata for key distribution, information is stored on keys by which content encrypting is done; it is distributed simultaneously with the distribution of content that is treated the same as metadata for storage/playback. In the metadata list are stored information for updating the metadata for the EPG [electronic program guide] stored by using it together with the PSI/SI, and information for acquiring necessary data from the stream group during distribution; it is distributed at all times to all reception terminals, without distinction of users who use reception terminals. In metadata for system key updating is stored information for updating the common key for the entire system that is previously stored within the terminals; it is distributed, unsynchronized with the distribution of the content, to all reception terminals, without distinction of users who use reception terminals.

[0021] (Encryption method) Next we describe the encryption method for content and metadata in this comprehensive data distribution service. The encryption method for content and metadata in this comprehensive data distribution service is different from the method by which encryption is done at the time of distribution in a conventional digital broadcast, because encrypted content and encrypted metadata are stored without decryption; it is a method in which the encryption is done when the content and metadata are generated.

[0022] Figure 4 is an explanatory diagram comparing the encryption methods of the comprehensive data distribution service and an existing service. Using Figure 4, we compare the encryption method in this comprehensive data distribution service and the encryption method in conventional digital broadcasting. In the conventional method, content is generated 20, and before encrypting the content that is generated, TSP 21 is formed, which is a data form at the time of distribution, so it is split into blocks, a part 23 of the divided-into-blocks content is stored in the payload part 22 of the TSP, and because thereafter the payload part of the TSP is encrypted 24, when the content is assembled on the reception terminal side, it is necessary to decrypt the payload part. On the other hand, in the case of the encryption method in this comprehensive data distribution service, the encryption 25 of the content takes place on the transmission side after generation 20 of the content, the encrypted content is divided into blocks, block 26 of part of the encrypted content divided into blocks in the payload part 22 of the TSP is stored and distributed, so if the content is assembled on the reception terminal side, the payload part can be assembled without decryption, and content and metadata can be stored on the transmission side in still encrypted form.

[0023] (Encryption method for content and metadata) Figure 5 is an explanatory diagram of the encryption method for content. And Figure 6 is an explanatory diagram of the encryption method for metadata. Next, using Figure 5 and Figure 6, respectively, we describe the encryption method for content and for metadata. In the encryption of content in this comprehensive data distribution service, each element that constitutes each content is encrypted regardless of which type it is, image content 27, or data content 28. For example, if image content 27 consists of two elements, MPEG2-Video (PES) 29 and MPEG2-AAC (PES) 30, all the data in each element is encrypted, generating encrypted elements 31 and 32. What is used for the encryption key 33 for encryption at this time is the common encryption key Kk1 within the content. In this comprehensive data distribution service, this encryption key 33 that is allocated to each content is called the content key Kk1. Thus the elements that make up data content 28, which is separate from image content 27, are encrypted by a different encryption key 34. Similarly, at this time a common key Kk2 within the content is used for the encryption key 34. The content key Kk is the general term for content keys as a whole.

[0024] Encryption of the metadata in this comprehensive data distribution service, unlike encryption of the content, does not involve encryption of all the metadata that requires encryption; as in Figure 6, only the part 35 that requires encryption is extracted and encrypted, producing encrypted data 37 to which is added information on the quantity 36, etc.

of encrypted data. Also, in this comprehensive data distribution service, according to the operation, this encrypted data 37 could either be embedded once more into the unencrypted metadata 38 and be distributed, or it could be distributed as a separate file. Figure 51 is an explanatory diagram for the content, the encryption key used when encrypting each kind of metadata mentioned above, and encryption keys in this comprehensive data distribution service.

[0025] (Restricted reception method) Figure 7 is an explanatory diagram of the restricted reception method in a comprehensive data distribution service. Next, we refer to Figure 7 in explaining the restricted reception method in which only users having a contract with the broadcaster are allowed to receive/store the content of for-fee broadcasts, etc. The restricted reception method in this comprehensive data distribution service is different from the method in which it is done channel by channel and program by program for each terminal according to the method used in conventional digital broadcasting; by using metadata, restricted reception in content units is made possible for each user that uses a terminal. As stated above, a content unit is the unit intended by the broadcaster, so the smallest unit is the element unit, making possible restricted reception in such fine units as the individual scenes that make up a program. In the method in this comprehensive data distribution service, restricted reception is done by metadata for prior contract and metadata for key distribution.

[0026] First, a user on the reception side 200 makes to a fee-charging business on the transmission side 100 a contract request 39 including the terminal ID, personal ID, and the channel, program, and content, etc. he wishes to contract. On the transmission side 100, metadata for prior contract is generated according to the contract request made by the user, the parts of the contract information, etc. that require protection are encrypted with the terminal key Kmc that is unique to each terminal, and it is distributed 45 to each user on the reception side 200. At the reception terminal on the reception side 200, it is decided according to the terminal ID and personal ID stored in the unencrypted part of the metadata for prior contract 40 whether it is information addressed to the user who uses the terminal, and if an ID is stored that is addressed to the using user, the metadata for prior contract is decrypted by the terminal key Kmc 43 that is prestored inside the terminal, and contract information is obtained that consists of the fee-charging business ID, the business key Kw 44 unique to each business, and the contract code, etc. The user who obtains the contract information makes a request 46 for the content 17 that is next to be broadcast by the contract business. On the transmission side 100, synchronized with the distribution of the encrypted content 17, the encryption key Kk 33 of the content necessary when viewing the content is stored, and metadata for key distribution 41 whose necessary parts are encrypted with the business key Kw 44 is distributed to all the terminals. Also, on the transmission side 100, use restrictions information, etc. with respect to the content is stored, and metadata for storage/playback 42 whose necessary parts are encrypted with the content key Kk 33 is distributed to all the terminals. The reception terminal receives the metadata for key distribution 41 that is distributed simultaneously with the content and decides according to the fee-charging business ID that is stored in the unencrypted part whether it is a broadcast by the contract business; if it is decided that it is metadata for key distribution 41 with respect to the content to be broadcast by the business with which one will contract, then the encrypted parts are decrypted according to the business key Kw that was distributed by the metadata for prior contract 40, and it is decided according to the decrypted relevant contract code and the contract code distributed by the metadata for prior contract 40 whether it is content that can be used within the user's form of contract. Here, if it can be used, the content key Kk 33 is stored in the reception terminal, and the encrypted parts of the metadata for storage/playback 42 that is received at the same time are decrypted with the content key Kk 33, the age restrictions and other use restrictions information with respect to the content are confirmed, and if use by the user is allowed, then the encrypted content 17 can be received according to the encrypted content 17 distribution location information that is stored in the metadata for storage/playback 42. With this comprehensive data distribution service, restricted reception is made possible by the above method.

[0027] 2. Billing method

Next, we describe the billing system in this comprehensive data distribution service. In this comprehensive data distribution service, it is divided broadly into two kinds of billing: billing for prior contract, and billing for at the time of content viewing.

[0028] (Billing for prior contract) Figure 8 is an explanatory diagram of the method of billing by prior contract. First, using Figure 8 we explain billing for prior contract. Billing for prior contract is a billing method in which billing for a fixed amount can be done regardless of whether there is any content viewing by the user, because the billing is done based on customer information obtained by advance user registration 47 on the transmission side 100. A user who has purchased a reception terminal 3 gives the transmission side 100, by postcard or telephone, etc., information including the terminal ID, personal ID, the business he wants to contract with, the form of contract, and the term of the contract, as well as information including the bank account where payment is to be made 48. On the transmission side 100, based on this information, customer information is generated and managed, metadata for prior contract 40 is generated in which are stored a contract code indicating the form of contract and the effective term of the contract, etc., it is distributed to the reception terminal 3 of the contract user, and billing is done for a periodic content use contract by user's designated account, etc. 48. A user who has received metadata for prior contract 40 is able to use the content of the business contracted within the effective term that is stored. The foregoing is the flow of billing for prior contract in this comprehensive data distribution service.

[0029] (Billing for viewing contract) Next we explain billing for a viewing contract. In the billing method for a viewing contract in this comprehensive data distribution service, the billing is divided into billing that assumes an uplink on the transmission side from the reception side, such as a terrestrial circuit, and billing that does not assume an uplink.

[0030] (Billing method that does not assume an uplink) Figure 9 is an explanatory diagram of the method for billing for a viewing contract that does not require an uplink. First,

we refer to figure 9 in explaining the method of billing that does not assume a terrestrial circuit or other uplink. Billing that does not assume an uplink is a method in which a fixed-point use for example is paid in advance in the same way as in the case of a prior contract. But if the fixed point is exceeded, additional points can be contracted on each such occasion. As a specific means, as with billing for a prior contract, when a user who purchases a reception terminal gives notice to the transmitting side 100 of his terminal ID, personal ID, the business he wants to contract with, the form of the contract, and the bank account where payment is to be made 48, etc., he makes not a contract for a fixed term but a contract by giving notice of the number of points 49 for using content. On the transmission side 100, customer information is generated and managed based on this information, the number of points consented to is stored in the metadata for prior contract 40 instead of information concerning the effective term of the contract, and it is distributed to the contract user's reception terminal 3. Also on the transmitting side 100, when distributing content 17, information on the number of points needed when using the content is stored in metadata for storage/playback 42 that is distributed in synchronization, and is distributed. At the reception terminal 3, when using content, the required number of points that is stored in the metadata for storage/playback 42 is deducted from the number of points distributed according to the metadata for prior contract 40, and the content is played back, so content can be viewed in the range of the number of points distributed by the metadata for prior contract 40. On the transmission side 100, billing can be done in accordance with the content watched by the user, because billing can be done from a previously reported designated account, etc. 48 in accordance with the number of points permitted to the user. The number of points distributed according to the metadata for prior contract 40 is basically stored on a memory card, but in the case of points, etc. for a user group that uses reception terminals, it is also possible to store it in the reception terminals.

[0031] (Billing method that assumes an uplink) Next we describe the billing method that assumes that a terrestrial circuit 11 or other uplink is connected to the reception terminal 3. As expansions of the billing method with respect to the point of the previous paragraph in this comprehensive data distribution service, there exist a method in which asking for and adding points, etc. is possible by a terrestrial circuit 11, etc. connected to the reception terminal 3, and a method in which the billing information 50 when content is actually used on the reception terminal side is sent to the transmission side 100 over a terrestrial circuit 11, etc., and the billing is done based on this information.

[0032] Figure 10 is an explanatory diagram of an online billing method that employs an uplink. Here we refer to Figure 10 in describing the latter method according to the billing information 50. As a specific means for sending online billing information 50 to the transmission side 100 and doing the billing, similarly to the billing method described above, when a user who purchases a reception terminal 3 notifies the transmission side 100 of his terminal ID, personal ID, the business he wants to contract with, the form of the contract, and the account where payment is to be made 48, etc., rather than a contract for a fixed period and a fixed number of points, a contract is made for sending billing information 50 for the viewing of content online. In this comprehensive data distribution service, this contract is called an online PPV [pay per view] consent contract. On the transmission side 100, based on this information, customer information is generated and managed, and transmission destination information, etc. at the time of transmission of the billing information is stored in the metadata for prior contract 40 and is distributed to the contract user's reception terminal 3 as online PPV consent, rather than as information on the effective term of the contract, the number of points consented to, etc. Also, on the transmission side 100, information based on generating fee and other billing information 50 at the time of use that will be necessary when using the content is stored in the metadata for storage/playback 42 that is distributed in synchronization with when content 17 is distributed, and it is distributed. At the reception terminal, when the content is to be used, the using user's ID and other information is added to the information that is the basis for generating the billing information 50 that is stored in the metadata for storage/playback 40 [sic], and transmission takes place over terrestrial circuits to the transmission destinations designated by the metadata for prior contract 40. In this way, it is possible on the transmission side 100 to charge the fee within the billing information 50 transmitted by contract user's reception terminal 3 in accordance with the user's quantity of content viewing by the previously registered designated account, etc. 48.

[0033] 3. Service flow

Figure 11 is an explanatory diagram of flow of service in a comprehensive data distribution service. Next, we refer to Figure 11 in explaining the flow of service in this comprehensive data distribution service. This comprehensive data distribution service includes, for example, prior contract flow 105 at the time of user registration by a telephone or the postcard that is attached when the reception terminal 3 is purchased, content generation 102 on the transmission side 100, transmission-side flow 101 from metadata generation 103 to distribution 104, and reception-side flow 331 including content reception, playback, etc.

[0034] (Prior contract flow) Figure 12 is an explanatory diagram of the service flow in the prior contract. In the following we refer to Figure 12 in explaining the service flow in the prior contract. The prior contract flow 105 in a comprehensive data distribution service is for the purpose of doing customer information management 107 of service reception users 106 on the transmission side 100. In a comprehensive data distribution service, it is a service mainly for for-fee stored-type content, so a user needs a memory card 15 to make a content viewing contract, and the means by which a user acquires the memory card 15 is a prior contract. As explained above under restricted reception method and billing method, with a telephone call, etc. or the postcard that is attached at the time of purchase of a terminal, a user 106 on the reception side 200 registers on the transmission side 100, together with the name and address of the user 106, personal information concerning the user as an individual, including the bank account, etc. where payments are to be settled at the time of viewing a for-fee broadcast, etc., the for-fee services that he wants to watch, and the form of the contract, etc., along with the terminal ID or other information by which to identify the reception terminal. On the transmission side 100, a personal ID is assigned to the user

based on information including user-registered personal information, contract information, and the terminal ID and other information for identifying the reception terminal 3, and customer information is generated and managed 107. Also, on the transmission side 100, the personal ID and other information that is assigned based on this customer information is stored on a memory card 15, which is passed out to the user 106, and metadata for prior contract 40 in which is stored the contract code and other information indicating the key and mode of contract of the business with which the user 106 who has the memory card has made a contract is distributed to the reception terminal 3 and to the memory card 15 that has been passed out. At this point, the user 106 can avail himself of the contracted content, and management of the customer information of the contract user can be done on the transmission side 100.

[0035] (Transmission-side flow) Figure 13 is an explanatory diagram of the service flow on the transmission side. In the following, we refer to Figure 13 in describing the service flow on the transmission side. The flow of service on the transmission side in a comprehensive data distribution service includes, for example, content generation 102, program scheduling 208, content encryption 209, distribution formatting 212, PSI/SI generation 210, metadata generation 103, metadata encryption 211, and distribution 104.

[0036] Content generation 102 refers to generating content 1 from video/audio/data elements. Program scheduling 208 means producing broadcast programs by putting together one or multiple items of generated content. Content encryption 209 means generating encrypted content 17 by encrypting by the content key Kk, which is the key for each content, the elements that are included in the various content that is made into a program. Distribution formatting 212 means converting encrypted content 17 and encrypted metadata according to the types of the elements into TSP, which is the data format at the time of distribution. PSI/SI generation 210 means generating a PSI/SI table 19 based on program operation information, etc. generated by doing program scheduling 208. Metadata generation 103 means generating various metadata including a metadata list 250, metadata for EPG 251, metadata for storage/playback 252, and metadata for key distribution 253, according to the content at the time of content generation 102 and program scheduling 208, information on a program's title, nature, composition, and use restrictions, the encryption method in content encryption 209, information on encryption keys, etc., and information on distribution positions, etc. along the transmission channel when distribution formatting 212 is done. Metadata encryption 211 means generating metadata for encrypted EPG 254, metadata for encrypted storage/playback 255, and metadata for encrypted key distribution 256, by doing encryption on the parts that require protection in the various metadata generated by metadata generation 103. Distribution [sic; no 'formatting'] 212 means multiplexing and distributing to the reception side the PSI/SI, various metadata, and encrypted content.

[0037] (Reception-side flow) Figure 14 is an explanatory diagram of the service flow on the reception side. Service flow on the reception side in a comprehensive data distribution service includes reservations 332, content reception/storage 333, viewing contract 334, and playback 335. Reservations 332 means making reservations for desired content using metadata for EPG 254 distributed by the transmitting side 100. Content reception/storage 333 means receiving metadata for storage/playback 255, metadata for key distribution 256, and encrypted content 17 at the time of content distribution based on reserved information, and storing metadata 4 storage/playback 255 and the encrypted content 17. Viewing contract 334 means making a viewing contract for content based on stored use restrictions information of metadata for storage/playback, personal information on the memory card 15, and contract information, etc. Playback 335 means deciding based on the information for making a viewing contract whether playback of the content is allowed, etc., decoding the encoded content 17, then playing back the content.

[0038] 4. Transmission-side system

Next we describe the transmission-side system for realizing these service flows.

Composition of the transmission-side system

Figure 15 is a block diagram of the composition of the transmission-side system as a whole. Referring to Figure 15, we describe the overall composition of the transmission-side system in a comprehensive data distribution service. The transmission-side system, as stated above, has a distribution center 220 that generates, encrypts, and distributes content and metadata, a key management center 240 that generates and manages keys and IDs to be used in the comprehensive data distribution service system, a customer management center 260 that generates and manages users' personal information and contract information and other customer information based on users' registered information, a terrestrial circuit management center 214 that manages connections by a terrestrial circuit 11 at the time of bidirectional communication service use such as requests and viewing history information/billing information from the user, and a physical distribution management center 213 that manages physical distribution of merchandise, etc. to users and sales outlets using distribution or a physical distribution network 12. We describe in detail the distribution center 220, key management center 240, and customer management center 260, which are particularly important in realizing the comprehensive data distribution service in this invention.

[0039] (1) Composition of the distribution center

Figure 16 is a block diagram of the composition inside the distribution center. Referring to Figure 16, we describe the composition inside the distribution center 220. The distribution center 220 has an authoring system 221 that produces content; a program composition management system 222 that puts together programs from content produced by the authoring system 221; a metadata generation device 223 that generates various metadata based on the information of the titles and composition of content and programs generated by the authoring system 221 and the program composition management system 222 when content is generated and when programs are put together; a PSI/SI generation device 224 that generates PSI/SI based on the operation schedule, etc. generated by the program composition management system 222; a content encryption device 225 that encrypts the elements within the content from which programs are put together by the program composition management system 222; a metadata encryption device 226 that encrypts the metadata generated by the metadata generation device 223; and a transmission system 227 that

multiplexes the data input by the PSI/SI device 224, the content encryption device 225, and the metadata encryption device 226, etc. and converts it to a format that can be distributed. In the following we describe the composition of each of these.

[0040] (Authoring system) Figure 17 is a block diagram of the composition inside the authoring system. Referring to Figure 17, we describe the authoring system 221, which generates content. The authoring system 221 is a system that handles the generation and management of content 1; it passes on to the program composition management system 222 a related file 233 in which is stored completed content and information on the title, nature, and composition, etc. concerning the content that is generated when the content is generated. As to the composition of the authoring system 221, it has an image authoring tool 228 that produces and edits elements of images, sound, and data; an audio authoring tool 229; a data authoring tool 230; a content composition device 231 that composes content 1 from the elements output by the authoring tools and generates a related file 233; and a content management server 232 for storing and managing the content and related file 233 that are generated by the content composition device.

[0041] The authoring tools of the image authoring tool 228, audio authoring tool 229, and data authoring tool 230 have functions including video capture and scanning functions to digitize VHS videos, Laser Disks (registered trademark), and photographs and other analog material input 234, the function of converting DAT, CD, DVD, and other digital material input 234 to a format that can be displayed by the reception terminal on the reception side, the function of editing digital materials, and the function of digital output of elements produced and edited for the content composition device 231. The content composition device 231 composes content 1 from one or multiple elements output by the authoring tools, and at the same time has the function of storing in the content management server 232 a related file 233 it generates by inputting the title of the content, the content ID, the nature of the content, its genre, use restrictions information such as copying restrictions, the intended age group, and copyrights, and information such as the data form and capacity, etc. of the constituent elements. The content management server 232 notifies the program composition management system 222 of completion of the content, and if there is a request from the program composition management system 222 to transfer the content and related file 233, it has the function of passing the requested content 1 and related file 233 to the program composition management system 222. But the content management server 232 also has the function of forcibly passing the content 1 and related file 233 to the program composition management system even if there is no transfer request from the program composition management system 222.

[0042] (Program composition management system) Figure 18 is a block diagram of the composition inside the program composition management system. Referring to Figure 18, next we describe the program composition management system 222. The program composition management system 222 is a system that composes programs from content generated by the authoring system 221, and puts together programs by generating and managing the operation schedule, etc. for the programs it composes. The program composition management system 222 has a program composition device 235 that composes content from content 1 input from the content management server 232 within the authoring system 221; a program operation schedule generation device 236 that generates and allocates an operation schedule 238 to the programs that are composed; and a program management server 237 that stores and manages a set of content organized into a program, a set of related files corresponding thereto, and the operation schedule. Also, the files in which information is assembled that relates to content in the generation of content in Figures 17 and 18 are referred to generically as content-related information, and a file in which this is stored is a related file 233.

[0043] The program composition device 235 composes programs from one or multiple content 1 and a related file 233 by the content management server 232, and it has the function of adding to the related file 233, which is input by the content management server 232, information with respect to the set of content as a program and with respect to the program, as well as information such as for example the program title, the program ID, the nature of the program, its genre, the ID of the business that will broadcast it, information concerning the contract, information concerning billing, and information on the composition of the content within the program. The program operation schedule generation device 236 allocates to the program that is stored in the program management server 237 information concerning the date and time of the broadcast and the channel, etc., generates the operation schedule 238, and stores it in the program management server 237. The program management server 237 has the function of storing and managing the content 1, related file set 233, and operation schedule 238, etc. that are input by the program composition device 235 and the program operation schedule generation device 236, and, based on the information of the operation schedule 238, inputting the operation schedule 238 and the related file set 233 into the metadata generation device 223 and the PSI/SI generation device 224, and inputting into the content encryption device 225 the content set and content ID set that corresponds to the program information that is input into the metadata generation device 223 and the PSI/SI generation device 224.

[0044] (PSI/SI generation device) Figure 19 is an explanatory diagram of the PSI/SI generation device. Referring to Figure 19, we describe the PSI/SI generation device 224. The PSI/SI generation device 224 has the function of generating the PSI/SI tables in conformity with the MPEG2-System according to the operation schedule 238 and related file set 233 that are input by the program management server 237 inside the program composition management system 222, and inputting the PSI/SI tables, converted to TSP, into the transmission system 227 based on the operation schedule information.

[0045] (Metadata generation device) Figure 20 is an explanatory diagram of the metadata generation device. Referring to Figure 20, next we describe the metadata generation device 223. The metadata generation device 223 has the function of generating the metadata list 250, the metadata for EPG 251, the metadata for key distribution 253, and the metadata for storage/playback 252 based on the

related file set and operation schedule input by the program management server 237 in the program composition management system 222, the content key Kk obtained by passing the ID of the content to the key management center 240, and the distribution position information, etc. in the transmission channel of the content, etc. input by the transmission system 227; outputting the metadata list to the transmission system 227; and outputting the other metadata to the metadata encryption device 226. The distribution position information in the transmission channel of the content, etc. that is input by the transmission system is sometimes taken to be unnecessary if the designation, etc. of a module is possible where it is the distribution position.

[0046] (Content encryption device) Figure 21 is an explanatory diagram of the content encryption device. Referring to Figure 21, we describe the content encryption device 225 in this system. The content encryption device 225 has the function of notifying the key management center 240 of the ID (content ID) input by the program management server 237 based on the content set and ID (content ID) set input by the program management server 237 in the program composition management system 222, receiving the relevant content key Kk, encrypting the corresponding elements in the content by the content key Kk as in the content encryption method referred to above, and outputting the encrypted content that is generated to the transmission system 227.

[0047] (Metadata encryption device) Figure 22 is an explanatory diagram of the metadata encryption device. Referring to Figure 22, next we describe the metadata encryption device 226. The metadata encryption device 226 has the function of encrypting the metadata for EPG 251 input by the metadata generation device 223, the metadata for storage/playback 252, the metadata for key distribution 253, and the metadata for prior contract 259 input by the customer management center 260 according to the encryption key information input from within the key management center 240, and outputting the generated encryption metadata to the transmission system 227.

[0048] In the following, we describe the encryption method for each kind of metadata. With regard to the metadata for EPG 251, encryption is done on the necessary parts by a system key Ksy 264 that is common to all reception terminals and is obtained by passing to the key management center 240 the system ID that is stored in the metadata for EPG 251. With regard to the metadata for storage/playback 252, encryption is applied to the necessary parts by a content key Kk 33 that is unique to the content and is obtained by passing to the key management center 240 the content ID that is stored in the metadata for storage/playback 252. With regard to the metadata for key distribution 253, the ID stored in the metadata is encrypted as follows. That is, if it is metadata for key distribution 257 with respect to free content, encryption is done on the necessary parts by a system key Ksy 264 that is obtained by passing the system ID to the key management center 240. And if it is metadata for key distribution 258 with respect to for-fee content, the business ID is encrypted with respect to the respective necessary parts by the business key Kw 44. With regard to metadata for prior contract 259, the necessary parts are encrypted by a terminal key Kmc 43 obtained by passing to the key management center 240 the terminal ID that is stored in the metadata for prior contract 259.

[0049] The result is that the generated encrypted metadata for EPG 254, encrypted metadata for storage/playback 255, encrypted metadata for key distribution (free) 261, encrypted metadata for key distribution (for fee) 262, and encrypted metadata for prior contract 263 are output to the transmission system 227.

[0050] (Transmission system) Figure 23 is a block diagram of the composition inside the transmission system. In the following, referring to Figure 23, we describe transmission system 227 in a comprehensive data distribution service. The transmission system 227 is a system that takes the PSI/SI, encrypted content, metadata, and other data input from the PSI/SI generation device 224, content encryption device 225, metadata encryption device 226, and metadata generation device 223, and assembles it into data that can be distributed to a reception terminal 3. The transmission system 227 has a carrousel generation device 239, a packetizer 241, a multiplexer (MUX) 242, and entrusted broadcasting equipment 243. The carrousel generation device 239 has the function of modularizing the various data for generating a data carrousel in the MPEG2-system according to the data encrypted content input by the content encryption device 225, the various encrypted metadata input by the metadata encryption device, and the metadata list input by the metadata generation device, then converting it to DII and DDB, and outputting it to the packetizer 241. The packetizer 241 has the function of taking the MPEG2-Video PES, MPEG2-Audio PES, and other image encrypted content input by the content encryption device and the DII, DDB, and other data input by the carrousel generation device, splitting it into TSP-format data, and outputting it to a multiplexer (MUX) 242. The multiplexer (MUX) 242 has the function of applying multiplexing to the TSP input by the PSI/SI generation device 224 and the packetizer 241 under transmission rate and other conditions, generating TS, and outputting it to the entrusted broadcasting equipment 243. The entrusted broadcasting equipment 243 has the function of further multiplexing the multiple TS input by the multiplexer (MUX) 242, making it into a data form that can be distributed to a reception terminal 3, and distributing it by a transmission antenna. The foregoing is the composition inside the distribution center 220 in this comprehensive data distribution service, and the function and data generation flow of the constituent devices.

[0051] (2) Key management center composition

Figure 24 is a block diagram of the composition inside the key management center. Referring to Figure 24, next we describe the key management center 240. The key management center 240 is a system that generates encryption keys for each ID registered by the distribution center 220 and the customer management center 260 and receives encryption keys passed in answer to requests for encryption keys from the various centers. The key management center 240 has a key generation device 244 and a key management server 245.

[0052] (Key generation device) Figure 25 is an explanatory diagram of the key generation device. Referring to Figure 25, next we describe the key generation device 244 in the key management center 240. The key generation device 244 has the function of generating, by the multiple content IDs 246 input by the metadata generation device 223 in the distribution center 220, content keys Kk 33 that are content encryption keys that correspond to the respective IDs, and

outputting the generated content keys Kk 33, together with the content ID 246, to the key management server 245. Also, the system key Ksy 264, the business key Kw 44, the terminal key Kmc 43, and the personal key Km 265 are generated by directly designating the system ID 247, the business ID 248, the terminal ID 249, and the personal ID 270, which are IDs for encryption keys within the key generation device 244, and are output, together with the IDs, to the key management server 245..

[0053] (Key management server) Figure 26 is an explanatory diagram of the key management server. Referring to Figure 26, next we describe the key management server 245. The key management server 245 has the function of managing the keys and IDs generated by the key generation device 244 and passing along encryption keys in response to requests for encryption keys by the content encryption device 225 in the distribution center 220, the metadata encryption device 226, the metadata generation device 223, and the customer information management server 267 in the customer management center 260. For example, if a content ID is passed along as a request for an encryption key by the content encryption device 225 in the distribution center 220, its function is to pass along a content key Kk that is an encryption key that corresponds to the content ID.

[0054] (3) Customer management center composition

Figure 27 is a block diagram of the composition inside the customer management center. Referring to Figure 27, next we describe the customer management center in this comprehensive data distribution service system. The customer management center 260 is a system that generates customer information based on the user registration information from the user 106, generates a memory card and metadata for prior contract according the encryption key and other information transferred by the key management center 240, distributes memory cards to users 106, and transfers metadata for prior contract to the distribution center 220. The customer management center 200 has a customer generation system 266 and a customer information management system 271.

[0055] (Customer information generation system) Figure 28 is a block diagram of the composition inside the customer information generation system. Referring to Figure 28, we describe the customer information generation system 266 in the customer management center 260. The customer information generation system 266 is a system that generates customer information according to prior contract and other information resulting from the user 106 doing user registration of the prior contract, etc. by the attached postcard or a telephone call at the time of purchase of the terminal, and outputs it to the customer information management system 271; it has a user interface 268 and a customer information generation device 269. The user interface 268 has the function of receiving user registration information from the user by postcard or telephone, etc. and putting the registered information into electronic form. The customer information generation device 269 has the function of editing, through user interface 268, the user registration information into customer information in a data form that can be recognized by the customer information management system 271, and outputting it to the customer information management system 271.

[0056] (Customer information management system) Figure 29 is a block diagram of the composition inside the customer information management system. The customer information management system 271 is a system that, based on customer information input by the customer information generation system 266, makes a request to the key management server 245 in the key management center for the personal ID 270 and personal key 265, etc., uses the personal ID 270 and personal key 265, etc. that it receives, and generates metadata for prior contract 40, a memory card 15, etc. The customer information management system 271 has a customer information management server 267, a memory card generation device 272, and a metadata for prior contract generation device 273.

[0057] The customer information management server 267 manages the customer information generated by the customer information generation system 266, generates user information 150 for receiving from the key management server 245 information including the personal key Km 265 and the business key Kw by which the user makes a contract. The user information 150 indicates, for the reception-side reception terminal to which a given terminal ID has been assigned, how many users use it, and with which broadcasters the users who use the terminal will make a contract. According to this user information 150, the key management server 245 can secure as many personal IDs 270/personal keys Km 265 to manage as there are users stored in the user information, and likewise can pass on to the customer information management server 267 terminal keys Kmc 43 that correspond to the terminal IDs 249 stored in the user information and business keys Kw that correspond to the business IDs with which users will make a contract. By adding to the customer information the personal ID 270, personal key Km 265, terminal ID 249, terminal key Kmc 43, business ID, and business key Kw that it receives, the customer information management server 267 will be able to ascertain such information as the terminal used by a user, personal information on the user himself, and contract information, and will be able to perform customer management. The memory card generation device 272, based on the customer information in the customer information management server 267, stores the personal ID 270, personal key Kmc 265, terminal ID 249, and users' personal contract information, including their names, telephone numbers, and dates of birth, in the prescribed area in an empty memory card, and distributes them to users 106. Like the memory card generation device 272, the metadata for prior contract generation device 273 generates, and passes on to the metadata encryption device 226 inside the distribution center, metadata for prior contract in which are stored, according to the customer information in the customer information management server 267, the IDs of businesses with which users will contract, business keys Kw, contract codes indicating the form of contract, personal IDs 270 assigned to users, and the IDs 249 of the reception terminals used by users. The foregoing is the composition of the transmission-side system and the data flow between devices.

[0058] (Information generated and distributed on the transmission side) Next we describe the various metadata that is generated on the transmission side and is distributed to reception terminals. The method for describing the metadata in this comprehensive data distribution service can be the

description in XML or other text form discussed above in Figure 6, or a description in binary form such as PSI/SI. But for parts that require encryption, the description is made in binary form in particular, for sake of improvement in interpreting and processing the description within a reception terminal, but if a reception terminal has high processing performance, it can also operate by descriptions in text form, in the same as with the unencrypted parts. We describe the meaning and composition of the various types of metadata.

[0059] (Metadata for prior contract) Figure 30 is an explanatory diagram of the metadata for prior contract and the information that is stored in it. First, referring to Figure 30, we describe the metadata for prior contract. The metadata for prior contract 263 is data that includes, as stated above, the business key Kw of a fee-charging business and the contract code and other information concerning the form of contract, and it is used for making decisions, primarily when restricted reception is done; it is metadata that is distributed when a terminal is purchased, when a contract is updated, when a business key Kw is updated, etc. It includes user identification information 275, whereby the reception terminal of a terminal ID, personal ID, etc. identifies whether it is data sent to the user who uses the terminal; encryption information 276 concerning encryption involving metadata such as the metadata's encryption method, encrypted parts, and ID (terminal ID) indicating the encryption key; password and other personal information 277 of the user himself; and contract information 278 including the ID of the contract business with which the user has a contract, the business key Kw, the effective term of the contract, the contract code, and the contract points. Falling under the encrypted parts are the personal information 277, in which is stored information such as where payments are made by each user, and the contract information 278, in which is stored information such as the business key Kw; encryption is done on the transmission side with the key Kmc 43 that is unique to the terminal used by the user, and this information is distributed to the reception terminal. For encryption keys that use encryption, depending on the operation, one can also use a personal key Km. Also, depending on the operation, apart from the above information, one can also store metadata attribute information, which is discussed below, in the metadata for prior contract.

[0060] (Metadata for EPG) Figure 31 is an explanatory diagram of the composition of the metadata for EPG and the information that is stored in it. Referring to Figure 31, next we describe the metadata for EPG 254. The metadata for EPG 254, which is mainly metadata to allow the user to check the content to be distributed and make reservations for viewing/storing the content to be distributed, includes metadata attribute information 279, including the metadata ID, metadata type, metadata size, etc. for recognizing different metadata in which the distribution time of the metadata for EPG overlaps with the distribution time of metadata for storage/playback and metadata for key distribution; encryption information 276 concerning the encrypted parts of metadata in the same way as metadata for prior contract; program information 280 concerning programs, including the program ID, the scheduled broadcast date and time, the nature of the program, the genre, the composition of the content, and the size of the program; content information 281 on the content ID, the nature of the content, and the composition of its elements, etc.; and use restrictions information 282, including the users who use the content, and information on the restrictions on the content itself, such as age restrictions, copying restrictions, and storage restrictions. With regard to the encrypted parts, copying restrictions and other use restrictions information 282 applies, and because the metadata of all users is available, it is encrypted and distributed on the transmission side according to the system key Ksy 264 that is common to all reception terminals. With regard to the content information 281, it can be distributed without storage, according to the EPG operation level in the comprehensive data distribution service. Similarly with regard to the use restrictions information, sometimes operations are carried out without storage, and the metadata for EPG can be distributed without encryption.

[0061] (Metadata for storage/playback) Figure 32 is an explanatory diagram of the composition of the metadata for storage/playback and the information that is stored in it. Referring to Figure 32, next we describe the metadata for storage/playback 255. The metadata for storage/playback 255 is metadata that includes information needed for receiving content, storing it, and playing it back; besides being used when retrieving stored content, it is used for controlling how the user's content is used. The metadata for storage/playback includes metadata attribute information 279 for identifying the metadata itself, as with metadata for EPG; encryption information 276; program information 280; content information 281; use restrictions information 282; contract information 284, including the encryption method of the content shown by the metadata for storage/playback, encryption key ID and other content encryption information, and information for viewing content, as well as the form of the contract and usable time periods according to the contract; and billing information 285 including billing fees under the contract, the billing timing, etc. The encrypted parts include the use restrictions information 282, the content encryption information 283, in which the content encryption method, the encryption key ID, and other information is included, the contract information 284, in which use restrictions time periods and other information is included, and the billing information 285, in which the fees and timing for billing are included; the key by which the content is encrypted is encrypted by the same content key Kk 33 on the transmission side and is distributed. And with regard to the content information 281 in the metadata for storage/playback, the content distribution position and other information is added to the content information that is stored in the metadata for EPG.

[0062] (Metadata for key distribution) Figure 33 is an explanatory diagram of the composition of the metadata for key distribution and the information that is stored in it. Referring to Figure 33, next we describe the metadata for key distribution 256. The metadata for key distribution 256 is metadata for distributing information concerning content encryption keys; if the content is a for-fee broadcast, information is included for carrying out restricted reception that can be received only by users who have made a contract with the broadcasting business. The metadata for key distribution 256 includes metadata attribute information 279 for distinguishing it from other metadata; encryption information 276 concerning the encryption of the metadata

itself; and content key information 286 with the content ID, the content encryption key Kk, and other information. The content key Kk and other content key information concerning the encrypted parts is encrypted and distributed on the transmission side. With regard to the encryption key, the metadata for key distribution 256 is metadata with respect to for-fee content; if restricted reception is done that can be received only by users who have contracted with the business, then the business key Kw 44 that is unique to each business is used, and in the case of metadata for free content that can be viewed even by users other information contracting parties, then the system key Ksy 264 that is common to all reception terminals is used. Also, the business ID, the relevant contract code, and other information for realizing restricted reception is stored in the content key information, is encrypted, and is distributed.

[0063] (Metadata list) Figure 34 is an explanatory diagram of the composition of the metadata list and the information that is stored in it. Referring to Figure 34, next we describe the metadata list 250. The metadata list is metadata for acquiring the distribution position, within the distribution stream, of the metadata for EPG, the metadata for storage/playback, etc.; it holds information that supplements the PSI [program-specific information] and includes information for difference metadata storage if metadata for EPG in the distribution stream is updated with respect to metadata for EPG that is stored in the reception terminal. The metadata list 250 includes metadata list attribute information 287, such as the version, for recognizing the updating of information on the reception terminal side; the ID of the metadata corresponding to the content ID; the metadata type for distinguishing metadata for EPG and metadata for storage/playback; the version of the metadata for recognizing the updating of the metadata for EPG, and position information in the distribution stream and other list information 288. The metadata list itself, being information for acquiring metadata from the distribution stream, has no particular need for protection, and is distributed without being encrypted. As the method for acquisition of the metadata stream, operation is adopted in which acquisition is done by designating the distribution stream within the PMT in the PSI table.

[0064] (Metadata for system key updating) Figure 35 is an explanatory diagram of the composition of the metadata for system key updating and the information that is stored in it. Referring to Figure 35, next we describe the metadata for system key updating. The metadata for system key updating 289 is metadata for updating to system key Ksy3 the system key Ksy that is the common key for all reception terminals that is stored in the reception terminal. The metadata for system key updating 289 includes metadata attribute information 279 for distinguishing it from other metadata, encryption information 276 concerning encryption of the metadata itself, and system key information 290, in which is included such information as the system ID corresponding to the system key to be updated, the system ID after updating, the system key, and the update timing.

[0065] Qualifying as an encrypted part is the system key information 290, in which is included information on the system key after updating and the timing of the change, and the encryption key that is used is the system key Ksy2 that is previously registered in the reception terminal as the spare system key. The system key Ksy is a generic term for system keys in general, and normally one is in effect. But a spare system key Ksy2 is used when damage such as hacking occurs. Thus normally two system keys Ksy1 and Ksy2 are built into the receiver. To specifically describe the updating process for a system key Ksy, we discuss the two system keys Key1 and Key2 that constitute the inside of the actual receiver of the system key Key. Key1 and Key2 are built into the interior of the receiver, and when these keys are updated or otherwise changed, the system key transmission side transmits another system key Key3 by satellite, and system key Ksy1 changes to Key3 at the reception terminal. Thus there exist two system keys Key2 and Key3 within the actual receiver. Also, system key Key2 is actually the effective key. The foregoing is the metadata that is distributed by the transmission side in this comprehensive data distribution service.

[0066] 5. Reception-side system

Next we describe the reception terminal, which is the reception-side system that carries out the above service flow.

(Composition of the reception terminal) Figure 36 is a block diagram of the composition inside the reception terminal. Referring to Figure 36, next we describe the reception terminal 3, which is the reception terminal in this comprehensive data distribution service. With an antenna 2, the reception terminal 3 receives information including content 17 via satellite, PSI/SI 19, and metadata 18; it is output on a monitor device such as the TV 9, and viewing by users is possible by outputting it after it has been stored in a storage medium 4. In the future this reception terminal 3 may be built into a TV 9 or other monitor device, but in this explanation, as an example, we treat it as a separate device. A major feature of the reception terminal 3 for a comprehensive data distribution service is that besides having a storage medium 4 for storing information such as content 17 and metadata 18, it has a memory card 15, which is a personal authentication device that decrypts data that is encrypted and distributed and encrypts important information that is generated within the reception terminal, carries out the RMP [Rights Management and Protection] 16 function concerning the handling and control of copyright protection and other rights, authentication, and billing, etc., and handles personal authentication of users who make use of this reception terminal, and group authentication of the family, etc. to which the user belongs. This RMP 16 function includes an RMP controller 306, which interprets metadata and controls processing concerning rights protection; a metadata decryption function 307, which decrypts encrypted metadata; a content decryption function 308 for decrypting encrypted content; a key management table 311, which manages the keys used within the reception terminal; a profile 310 for setting the environment of the user who uses the reception terminal; and a metadata encryption function 309, which encrypts data that requires protection, such as information for allowing the viewing of content generated by metadata within the reception terminal, etc. The storage medium 4 has a hard disk, which is a fixed, large-capacity storage medium in the reception terminal in which are stored, besides the aforementioned content 17 and metadata 18, information such as reservation information 313 generated within the reception terminal, and a search/EPG table 312, as well as removable media such as DVD-RAM and memory cards that

can be removed and that stores information such as necessary content and metadata. Stored on the memory card 15 are, besides the aforementioned personal ID 270, personal key 265, and personal contract information 274, consent information 314 that serves as decision data by which consent is given for viewing content generated within the reception terminal. RMP 16 may have a composition in which security is ensured by security measures against piracy and encryption-breaking, etc., but a composition may also be adopted in which modules can be replaced due to degradation of the strength of security, etc.

[0067] Next we describe RMP 16, storage medium 4, and memory card 15, which are characteristic functions of the reception terminal.

(RMP) The RMP 16 function in this comprehensive data distribution service includes an RMP controller 306, which interprets metadata and controls processing concerning rights protection; a metadata decryption function 307, which decrypts encrypted metadata; a content decryption function 308 for decrypting encrypted content; a key management table 311, which manages the keys used within the reception terminal; a profile 310 for setting the environment of the user who uses the reception terminal; and a metadata encryption function 309, which encrypts data that requires protection, such as information for allowing the viewing of content generated by metadata within the reception terminal, etc.

[0068] Figure 52 shows the main control processing carried out by the RMP controller 306. As depicted in the diagram, the main functions of the RMP controller 306 are, for example, reception control, storage control, copying control, presentation control, viewing contract control, billing control, personal authentication control, key management, profile management, time management, application authentication control, external equipment authentication control, and communication circuit control.

[0069] (Metadata decryption) Figure 37 is an explanatory diagram of the metadata decryption function. Referring to Figure 37, next we describe metadata decryption. The metadata decryption function 307 is a function that, upon the occurrence of a decryption request from the RMP controller 306, decrypts encrypted metadata, etc. using the encryption key passed via the RMP controller 306 according to the key management table 311. If at the time of content reception/storage or at the time of a content viewing contract, etc. it is judged that there is a need to decrypt the metadata, the RMP controller 306 first reproduces the encrypted metadata on the storage medium or the encoded personal contract information, etc. on the memory card, reads the encryption key ID in the aforesaid encryption information that is stored in the unencrypted part of the data, and passes the encryption key ID to the key management table 311. The key management table 311 identifies the corresponding encryption key corresponding to the encryption key ID that has been passed, and passes the encryption key to the RMP controller 306. The RMP controller 306 passes the encryption key passed from the key management table and the metadata to the metadata decryption function 307, and requests decryption. The metadata decryption function 307 extracts the encrypted part of the metadata that has been passed to it, decrypts the extracted encrypted part with the decryption key that has likewise been passed from the RMP controller 306, stores the prescribed part of the metadata of the unencrypted part, and passes it as decrypted metadata to the RMP controller 306. But sometimes, as stated above, depending on the operation, the data format for the decrypted part is different from the unencrypted part, so if that is the case, processing is carried out in which the subsequent operation is carried out without storing it. The foregoing is the decryption processing by the metadata decryption function 307. As the kinds of metadata that are decrypted by the metadata decryption function 307, we can list metadata for EPG 254, metadata for storage/playback 255, metadata for key distribution (free) 261, metadata for key distribution (for fee) 262, metadata for prior contract 263, and metadata for system key updating 289, plus personal contract information 274 and consent information 314, which are stored on a memory card. With regard to the information stored on the memory card, namely the personal contract information 274 and the consent information 314, because the encryption key is not stored in a key table, they are decrypted after first acquiring from the RMP controller the personal key Km 265 that is on the memory card.

[0070] (Content decryption) Figure 38 is an explanatory diagram of the content decryption function. Referring to Figure 38 we describe content decryption. The content decryption function 308 is a function that, in response to a decryption request by the RMP controller 306, decrypts the elements within the content 17 using the content key, which is the content encryption key passed from the key management table 311 via the RMP controller 306; this processing is done mainly when content is played back.

[0071] (Profiles) Figure 39 is block diagram of a profile. Referring to Figure 39, next we describe the profile. Profile 310 is a collection of personal contract information 274 generated within the RMP by the metadata for prior contract 263; because it is data that requires protection, it is stored in memory area (secure memory) 317 within RMP whose security is safeguarded, and it is used when a decision is made about content viewing/storage reservations or restricted reception. Profile 310 includes overall profile 315, in which is stored contract information, etc. with respect to all terminal users, and personal profile 316, in which is stored the contract information for each user.

[0072] (Key management table) Figure 40 is block diagram of the key management table. Referring to Figure 40, next we describe the key management table. Key management table 311 is a table in which are stored IDs and keys, which is information for passing the relevant key to an ID designated by the RMP controller 306, and because it consists of key data that requires protection, like the profiles it is stored in memory area (secure memory) 317 within RMP whose security is safeguarded.

[0073] (Metadata encryption) Figure 41 is an explanatory diagram of the metadata encryption function. Referring to Figure 41, we describe metadata encryption. The metadata encryption function 309 is a function that uses the personal key Km 265 on a memory card 15 to encrypt the relevant information when storing on the memory card 15, according to RMP 16, the personal contract information 274 that is generated by the metadata for prior contract and the content consent information 314 that is generated by the metadata for storage/playback.

[0074] (Storage medium) Figure 42 is an explanatory diagram of the state of storage of information stored in a storage medium. Referring to Figure 42, next we describe the state of storage of the data that is stored in the storage medium 4 in a reception terminal 3. As data to be stored in the storage medium 4, there are the metadata list 250, the metadata for EPG 254, the search/EPG table 312, the reservation information 313, the metadata for storage/playback 255, the content 17, and software such as the operating system (OS) and applications of other reception terminals. In this example, the storage medium 4 itself does not have a structure whose security is protected, so the data that requires protection in the data that is stored in the storage medium is stored in encrypted state. The metadata list 250 for receiving the metadata for EPG 254 and metadata for storage/playback 255, etc., the search/EPG table 312 that is generated by the metadata for EPG 254 and metadata for storage/playback 255 for the purpose of performing EPG display on the reception terminal and doing search processing, and the reservation information 313 for content viewing/storage reservation that is generated by the metadata for EPG 254 are data that are not considered to require any particular protection, so they are stored in the storage medium without encryption. But if protection is necessary in an operation, encryption is done with the terminal key Kmc, etc. that previously exists in the terminal. The metadata for EPG 254, the metadata for storage/playback 255, and the content 17, in which is stored content use restrictions information, etc., are stored in encrypted form on the transmission side, and when these items of data require processing, a copy is generated, and by decoding and using the copy, reencryption processing within the reception terminal can be dispensed with.

[0075] (Memory card) Figure 43 is an explanatory diagram of the composition inside a memory card. Referring to Figure 43, we describe the composition inside a memory card 15 that is used in a general data distribution service. The memory card 15 has inside it a memory area (secure memory) 317 whose security is protected, and an ordinary memory area (ordinary memory) 318. Stored in the ordinary memory area 318 is data that requires no protection or data that requires protection but is protected by encryption, while the information that is stored in the secure memory area 317 is information that is data that requires protection but cannot be kept on a memory card in encrypted state. Qualifying as information to be stored in the secure memory area 317 are personal ID 270 allocated to an individual user, and personal key Km 265, which is the corresponding encryption key, while what qualifies as data to be stored in the ordinary memory area 318 is personal contract information 274 and consent information 314 that are encrypted on the RMP 16 side. Also, if a personal ID 270 and personal key 265 stored in the secure memory area 317 are to the passed to RMP 16, the data is passed likewise using a secure transmission channel. A secure transmission channel is realized by using a public-key method, etc.

[0076] (Information generated on the reception terminal side) Next we describe the processing during the generation of various information generated in a reception terminal in a comprehensive data distribution service.

[0077] (Profile generation) Figure 44 is an explanatory diagram of profile generation processing. Referring to Figure 44, first we describe a profile generated by metadata for prior contract. Profile 310 is information generated within the RMP based on the metadata for prior contract 262. In the generation of profile 310, first, after the metadata for prior contract 263 received by the transmission side is decrypted by the metadata decryption function, it is decided by the RMP controller 306, according to the terminal ID and personal ID in the user identification information 275 of the metadata for prior contract 263, whether it is contract information for all terminals or rather contract information for each user, and according to the personal information 277 and contract information 278 decrypted by the metadata decryption function, only the necessary data is extracted, and the personal contract information 274 is generated. In addition, the personal contract information 274 is stored in the overall profile 315 and in the personal profile 317 in the security area 317 recognized by the user identification information 275, and thereby profile 310 is generated.

[0078] (Key management table) Figure 45 is an explanatory diagram of how the key management table is generated. Referring to Figure 45, next we describe the processing when the key management table is generated. Present in the key management table 311 are IDs and key information previously stored in it when the user purchased the reception terminal, and IDs and key information generated when the user received the service. As the previously stored information, there are the terminal ID 249, the terminal key Kmc 43, the system ID 247, and the system key Ksy 264. Also, the system key Ksy is a generic term for system keys in general, including system keys Ksy1 to Ksy3. In this example, two types of system ID and key exist: the ID and key information Ksy1 that are used for operation, and the spare ID and key information Ksy2 that are put to use when the system key is updated. Qualifying as parts that are generated or updated on the reception side are the system ID 247 when the system key is updated, the system key Ksy 264, the business ID 248, the business key Kw 44, the content ID 246, and the content key Kk 33. The IDs and key data that are generated are stored in the encrypted part in the metadata for system key updating 289, metadata for prior contract 263, and metadata for key distribution 256 that are received by the reception terminal, so after decryption by metadata decryption inside RMP 16, by being extracted from the various metadata by the RMP controller and stored in the secure memory area 317, the key management table 311 is generated.

[0079] (Search/EPG table) Figure 46 is an explanatory diagram of how the search/EPG table is generated. Referring to Figure 46, we describe the search/EPG table. The search/EPG table 312 is generated by making a copy within RMP according to the received metadata for EPG 254 and metadata for storage/playback 255, decrypting the various metadata by the metadata decryption function, then extracting the necessary items by the RMP controller and storing it in the prescribed position in the storage medium 4. The search/EPG table 312 is a collection of simple information of the metadata for EPG 254 and the metadata for storage/playback 255, which exist multiply in the storage medium. Also, because the search/EPG table 312 is information that is stored in the storage medium without encryption, it can be accessed directly from search applications and EPG applications on the reception terminal,

which can increase the reception terminal's search speed and EPG display speed.

[0080] (Reservation information) Figure 47 is an explanatory diagram of how reservation information is generated. Referring to Figure 47, next we describe the reservation information. The reservation information 313 is information that is generated within the RMP 16 according to the metadata for EPG 254 and the profile 310 in response to a viewing/storage request by the user; it is information that is stored in storage medium 4 without encryption. When a viewing/storage request arises from the user, the RMP controller 306 generates in the RMP a copy of the metadata for EPG 254 for the content that is the object of the viewing request, and the copied metadata for EPG is decrypted by the metadata decryption function. Then the RMP controller 306 decides, according to the use restrictions information of the decrypted metadata for EPG and the user's personal contract information for which a reservation request was made in the profile, whether a reservation for the content itself can be made, and whether the user's form of contract allows reservation of the requested content, following which it decides according to other reservation information 313 in the storage medium 4 whether there is no registered reservation, and whether the schedule allows a reservation to be made. Here, if a reservation can be made, then the RMP controller 306, according to the metadata for EPG 245 and the personal ID of the user who made the reservation according to his personal contract information, extracts the content ID, content size, scheduled broadcast date and time, etc., and the type of reservation according to the user request, generates reservation information 313, and makes the reservation by storing it in the prescribed location in the storage medium 4. Reservation information is generated in the same way also if automatic storage is done using the preferences of the user.

[0081] (Personal contract information on a memory card) Figure 48 is an explanatory diagram of how personal contract information is generated. Referring to Figure 48, next we describe the encryption process when personal contract information in the profile is stored onto a memory card. The personal contract information on a memory card 15 is basically the encrypted form of the personal contract information 274 that is stored in the profile in the secure memory area in the RMP 16. The RMP controller 306, upon recognizing that a memory card 15 has been inserted, reads the personal ID 270 on the secure area on the memory card 15 via a secure transmission channel, and identifies the relevant personal contract information within the profile. Next, if personal contract information is present on the memory card 15, the RMP controller 306 reads it, decrypts it by the metadata decryption function, confirms the version number stored in the unencrypted part of the mutual personal contract information, and if the version of the memory card is new, the personal contract information encrypted on the memory card side is copied into the RMP, and using the personal key Km 265 obtained by the memory card 15 via a secure transmission channel, the personal contract information is decrypted by metadata decryption, and the personal contract information in the relevant profile is updated. If, conversely, the version of the personal contract information 274 on the profile side is new, then the RMP controller 306 uses the personal key Km 265 that is obtained by the memory card 15 through a secure transmission channel, and after the necessary parts of the personal contract information are encrypted by the metadata encryption function 309, the personal contract information is updated by storing it in the prescribed position on the memory card 15.

[0082] (Consent information) Figure 49 is an explanatory diagram of how the consent information is generated. Referring to Figure 49, next we describe the consent information. The consent information 314 is rights information with respect to viewing content; it is generated within the RMP 16 by a copy of the personal contract information 274 on the memory card 15 and of the metadata for storage/playback 255 in the storage medium 4. When a user's viewing request for content occurs, the RMP controller 306 generates inside RMP 16 a copy of the metadata for storage/playback 255 that corresponds to that content, and decrypts the copied metadata for storage/playback 255 by means of the metadata decryption function. After the metadata for storage/playback is decrypted, the RMP controller 306 acquires the personal contract information 274 that was encoded by inside [sic] the memory card 15 and, through a secure transmission channel, the personal key Km 265, and decrypts the personal contract information 274 by metadata decryption. After the personal contract information is decrypted, the RMP controller 306 decides by the personal contract information and by the use restrictions information in the metadata for storage/playback 255 whether it is content that the user may view, and according to the form of viewing contract chosen by the user, it extracts the items that are required according to the contract information and billing information, etc. in the metadata for storage/playback, generates consent information 314, encrypts it by the metadata encryption function 309 using the personal key Km acquired from the memory card 15, then stores the encrypted consent information in the prescribed position on the memory card. Also, if processing is to be done within the reception terminal such as automatic storage reservation or change of the screen display according to the user's preferences, processing can be done by assembling information on genre, etc. within the consent information, thereby judging what the user's preferences are. The foregoing is the processing on the information generated within the reception terminal in a comprehensive data distribution service. The comprehensive data distribution service generates various information using the aforesaid various metadata distributed by the transmission side and the metadata distributed within the reception terminal, which is the reception side, and by using it, the content copyright and other rights of the broadcaster, user, etc. can be protected.

[0083]

[Effects of the invention] According to this invention, as detailed above, a data distribution service method can be provided that adds control information that makes stored-type broadcasting and the protection of content possible.

[Brief Explanation of the Drawings]

[Figure 1] Block diagram of the reception side of a comprehensive data distribution service.

[Figure 2] Block diagram of the overall system of a comprehensive data distribution service.

[Figure 3] Explanatory diagram of the rights protection method in a comprehensive data distribution service.

[Figure 4] Explanatory diagram comparing the encryption method in a comprehensive data distribution service and an existing service.

[Figure 5] Explanatory diagram of the content encryption method.

[Figure 6] Explanatory diagram of the metadata encryption method.

[Figure 7] Explanatory diagram of the restricted reception method in a comprehensive data distribution service.

[Figure 8] Explanatory diagram of a billing method according to a previous contract.

[Figure 9] Explanatory diagram of a billing method for a viewing contract that does not require an uplink.

[Figure 10] Explanatory diagram of an online billing method using an uplink.

[Figure 11] Explanatory diagram of the flow of service in a comprehensive data distribution service.

[Figure 12] Explanatory diagram of the service flow in a prior contract.

[Figure 13] Explanatory diagram of the service flow on the transmission side.

[Figure 14] Explanatory diagram of the service flow on the reception side.

[Figure 15] Block diagram of the overall system on the transmission side.

[Figure 16] Block diagram of the composition inside the distribution center.

[Figure 17] Block diagram of the composition inside the authoring system.

[Figure 18] Block diagram of the composition inside the program composition management system.

[Figure 19] Explanatory diagram of the PSI/SI generation device.

[Figure 20] Explanatory diagram of the metadata generation device.

[Figure 21] Explanatory diagram of the content encryption device.

[Figure 22] Explanatory diagram of the metadata encryption device.

[Figure 23] Block diagram of the composition inside the transmission system.

[Figure 24] Block diagram of the composition inside the key management center.

[Figure 25] Explanatory diagram of the key generation device.

[Figure 26] Explanatory diagram of the key management server.

[Figure 27] Block diagram of the composition inside the customer management center.

[Figure 28] Block diagram of the composition inside the customer information generation system.

[Figure 29] Block diagram of the composition inside the customer information management system.

[Figure 30] Explanatory diagram of the composition of the metadata for prior contract and the information that is stored in it.

[Figure 31] Explanatory diagram of the composition of the metadata for EPG and the information that is stored in it.

[Figure 32] Explanatory diagram of the composition of the metadata for storage/playback and the information that is stored in it.

[Figure 33] Explanatory diagram of the composition of the metadata for key distribution and the information that is stored in it.

[Figure 34] Explanatory diagram of the composition of the metadata list and the information that is stored in it.

[Figure 35] Explanatory diagram of the composition of the metadata for system key updating and the information that is stored in it.

[Figure 36] Block diagram of the composition inside the reception terminal.

[Figure 37] Explanatory diagram of the metadata decryption function.

[Figure 38] Explanatory diagram of the content decryption function.

[Figure 39] Block diagram of a profile.

[Figure 40] Block diagram of the key management table.

[Figure 41] Explanatory diagram of the metadata encryption function.

[Figure 42] Explanatory diagram of the state of storage of the information stored in the storage medium.

[Figure 43] Explanatory diagram of the composition inside a memory card.

[Figure 44] Explanatory diagram of how a profile is generated.

[Figure 45] Explanatory diagram of how the key management table is generated.

[Figure 46] Explanatory diagram of how the search/EPG table is generated.

[Figure 47] Explanatory diagram of how reservation information is generated.

[Figure 48] Explanatory diagram of how personal contract information is generated.

[Figure 49] Explanatory diagram of how consent information is generated.

[Figure 50] Explanatory diagram of the data that constitutes image and data content.

[Figure 51] Explanatory diagram for the content, the encryption key used when encrypting each kind of metadata mentioned above, and encryption keys in this comprehensive data distribution service.

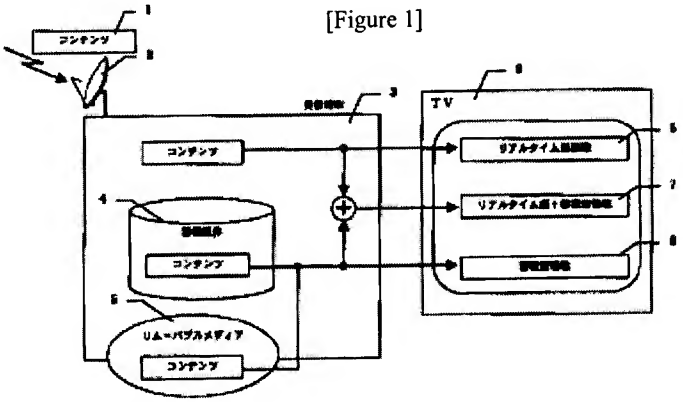
[Figure 52] Explanatory diagram of the main control processing done by the RMP controller 306.

[Explanation of the symbols]

1 ... content, 2 ... antenna, 3 ... reception terminal, 4 ... storage medium, 5 ... removable media, 6 ... real-time viewing, 7 ... real-time + stored-type viewing, 8 ... stored-type viewing, 9 ... TV, 10 ... satellite, 11 ... terrestrial circuit, 12 ... physical distribution network, 13 ... portable telephone network, 14 ... external devices, 15 .. memory card, 16 ... RMP, 17 ... encrypted content, 18 ... encrypted metadata, 19 ... PSI/SI, 20 ... content generation, 21 ... conversion to TSP, 22 ... payload, 23 ... part of the content, 24 ... encryption of the payload part, 25 ... content encryption, 26 ... part of the encrypted content, 27 ... image content, 28 ... data content, 29 ... MPEG2-Video (PES), 30 ... MPEG2-AAC (PES), 31 ... encrypted MPEG2-Video (PES), 32 ... encrypted MPEG2-AAC (PES), 33 ... Kk1, 34 ... Kk2, 35 ... encrypted necessary part, 36 encrypted data volume, 37 ... encrypted data, 38 ... unencrypted metadata, 39 ... contract request, 40 ... metadata for prior contract, 41 ... metadata for key distribution, 42 ... metadata for storage/playback, 43 ... terminal key Kmc, 44 ... business key Kw, 45 ... distribution to each user, 46 ...

content request, 47 ... user registration, 48 ... designated account, 49 ... point request, 50 ... billing information, 51 ... PPV registration, 100 ... transmission side, 101 ... transmission-side flow, 102 ... content generation, 103 ... metadata generation, 104 ... encryption/distribution, 105 ... prior contract flow, 106 ... user, 107 ... customer management, 150 ... user information, 200 ... reception side, 201 ... home, 202 ... vending machine, 203 ... sales outlet, 204 ... on-board terminal, 205 ... portable terminal, 206 ... portable telephone, 208 ... program scheduling, 209 ... content encryption, 210 ... PSI/SI, 211 ... metadata encryption, 212 ... conversion to distribution format, 213 ... physical distribution management center, 214 ... terrestrial circuit management center, 220 ... distribution center, 221 ... authoring system, 222 ... program composition management system, 223 ... metadata generation device, 224 ... PSI/SI generation device, 225 ... content encryption device, 226 ... metadata encryption device, 227 ... transmission system, 228 ... image authoring system, 229 ... audio authoring tool, 230 ... data authoring tool, 231 ... content composition device, 232 ... content management server, 233 ... related file, 234 ... material, 235 ... program composition device, 236 ... program operation schedule generation device, 237 ... program management server, 238 ... operation schedule, 239 ... carrousel generation device, 240 ... key management center, 241 ... packetizer, 242 ... MUX, 243 ... entrusted broadcasting equipment, 244 ... key generation device, 245 ... key management server, 246 ... content ID, 247 ... system ID, 248 ... business ID, 249 ... terminal ID, 250 ... metadata list, 251 ... metadata for EPG, 252 ... metadata for storage/playback, 253 ... metadata for key distribution, 254 ...metadata for encrypted EPG, 255 ... encrypted metadata for storage/playback, 256 ... encrypted metadata for key distribution, 257 ... metadata for key distribution (free), 258 ... metadata for key distribution (for fee), 259 ... metadata for prior contract, 260 ... customer management center, 261 ... encrypted metadata for key distribution (free), 262 ... encrypted metadata for key distribution (for fee), 263 ... encrypted metadata for prior contract, 264 ... system key Ksy, 265 ... personal key Km, 266 ... customer information generation system, 267 ... customer information management server, 268 ... user interface, 269 ... customer information generation device, 270 ... personal ID, 271 ... customer information management system, 272 ... memory card generation device, 273 ... metadata for prior contract data generation device, 274 ... personal contract information, 275 ... user identification information, 276 ... encrypted information, 277 ... personal information, 278 ... contract information, 279 ... metadata attribute information, 280 ... program information, 281 ... content information, 282 ... use restrictions information, 283 ... content encryption information, 284 ... contract information, 285 ... billing information, 286 ... content key information, 287 ... metadata list attribute information, 288 ... list information, 289 ... metadata for system key updating, 290 ... system key information, 300 ... service to the home, 301 ... service to vending machines/sales outlets, 302 ... service to mobile bodies, 303 ... package delivery service, 304 ... service to portable telephones, 306 ... RMP controller, 307 ... metadata decryption, 308 ... content decryption, 309 ... metadata encryption, 310 ... profile, 311 ...key management table, 312 ... search/EPG table, 313 ... reservation information, 314 ... consent information, 315 ... overall profile, 316 ... personal profile, 317 ... secure memory, 318 ... ordinary memory, 331 ... reception-side flow, 332 ... reservation, 333 ... content reception/storage, 334 ... viewing contract, 335 ... playback

[Figure 1]



1 content

content

3 reception terminal
6 real-time viewing
7 real-time + stored viewing

4 storage medium content

8 stored viewing

5 removable media content

[Figure 2]

100
Transmission side
- distribution center
- key management center
- customer management center
- terrestrial circuit management center
- physical distribution management center

11 terrestrial circuit

(4) package delivery service
DVD, etc.
12 physical distribution side

13 portable telephone side

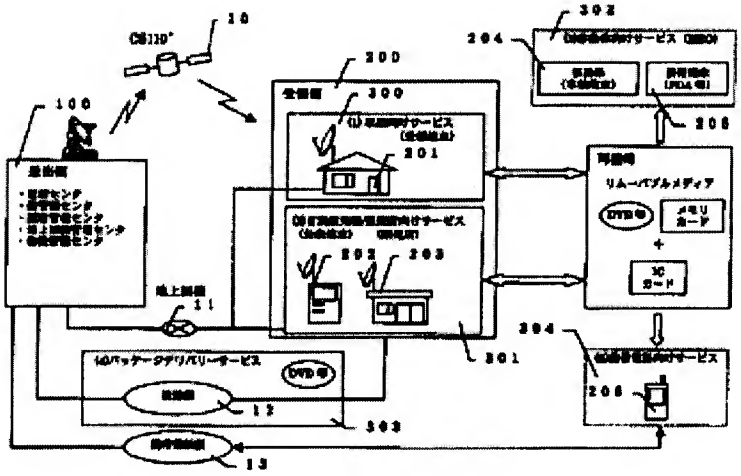
200 reception side

(1) service to the home (reception terminal)
(2) service to vending machines/sale outlets
(public terminal) (sales outlet)

302 service to mobile bodies (HEO)
204 mobile body (on-board terminal)
205 portable terminal (PDA, etc.)

transportable
removable media
DVD, etc. memory card
+
Memory card

304 (5) service to portable telephones



[Figure 3]

19 PSI/SI, etc. (1)
18 metadata (2)
17 encrypted content (3)

metadata reception control →
encrypted content →

reception terminal
viewing control → TV 9
RMP functions (4)
(including encryption/decryption functions)

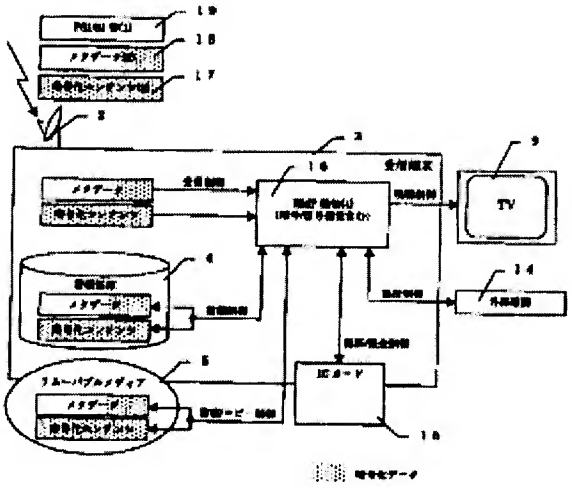
storage medium 4
metadata ← storage control
encrypted content ←

authentication control
→ external equipment 14

authentication/billing control
Memory card 15

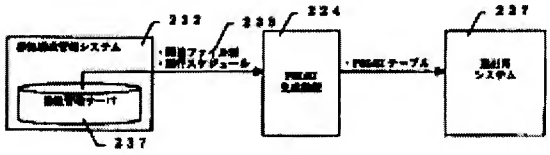
removable media 5
metadata ← storage/copy control
encrypted content ←

[shading] encrypted data



[Figure 19]

[left to right...]
program scheduling management system 222
program management server 237
233
- [illegible] file set
- operation schedule
PSI/SI generation device 224
- PSI/SI table
transmission system 227



[Figure 4]

(Previous method)

generation 20

content

TSP conversion 21

content 23

header [_____] 22

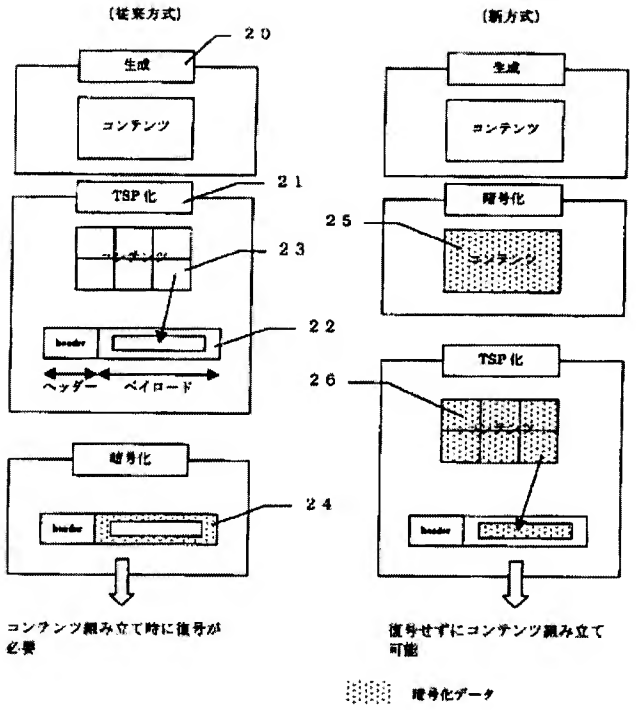
header payload

encryption

header [_____] 24

encryption needed when content is assembled

[shading] encrypted data



(New method)

generation

content

encryption

content 25

TSP conversion

content 26

header [_____]

content can be assembled without encryption

[Figure 14]

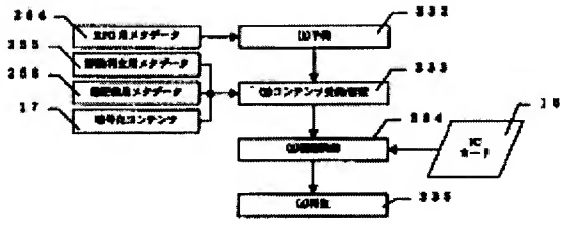
254 metadata for EPG
255 metadata for storage/playback
256 metadata for [illegible]
17 encrypted content

(1) reservation 332

(2) content reception/storage 333

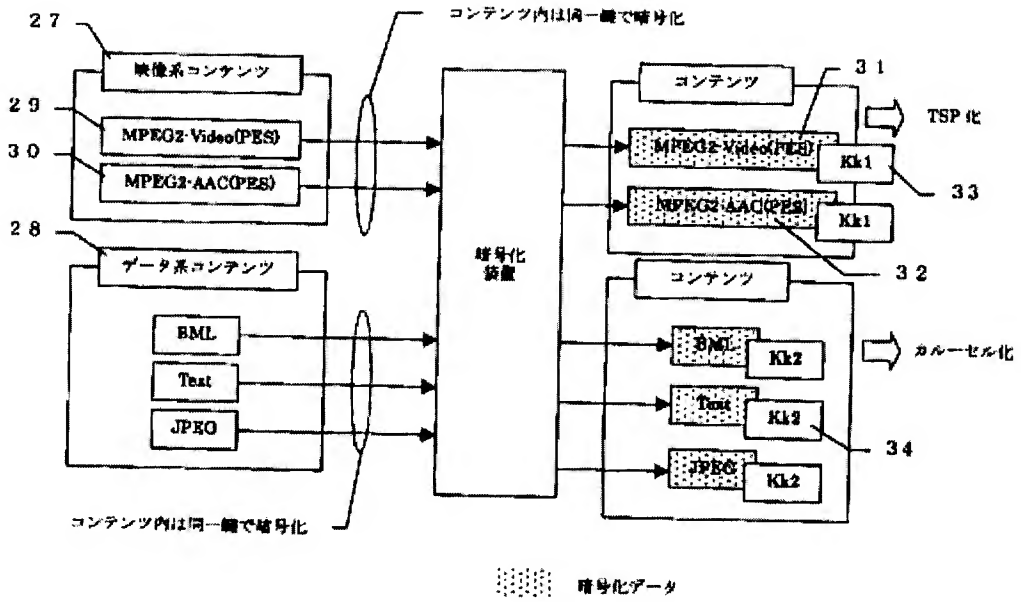
(3) viewing contract 334 ← Memory card 15

(4) playback 335



(23)

[Figure 5]



Within content, encrypted by same key

27 image content

content

⇒ TSP conversion

encryption device

28 data content

content

BML ...

⇒ carrouselization

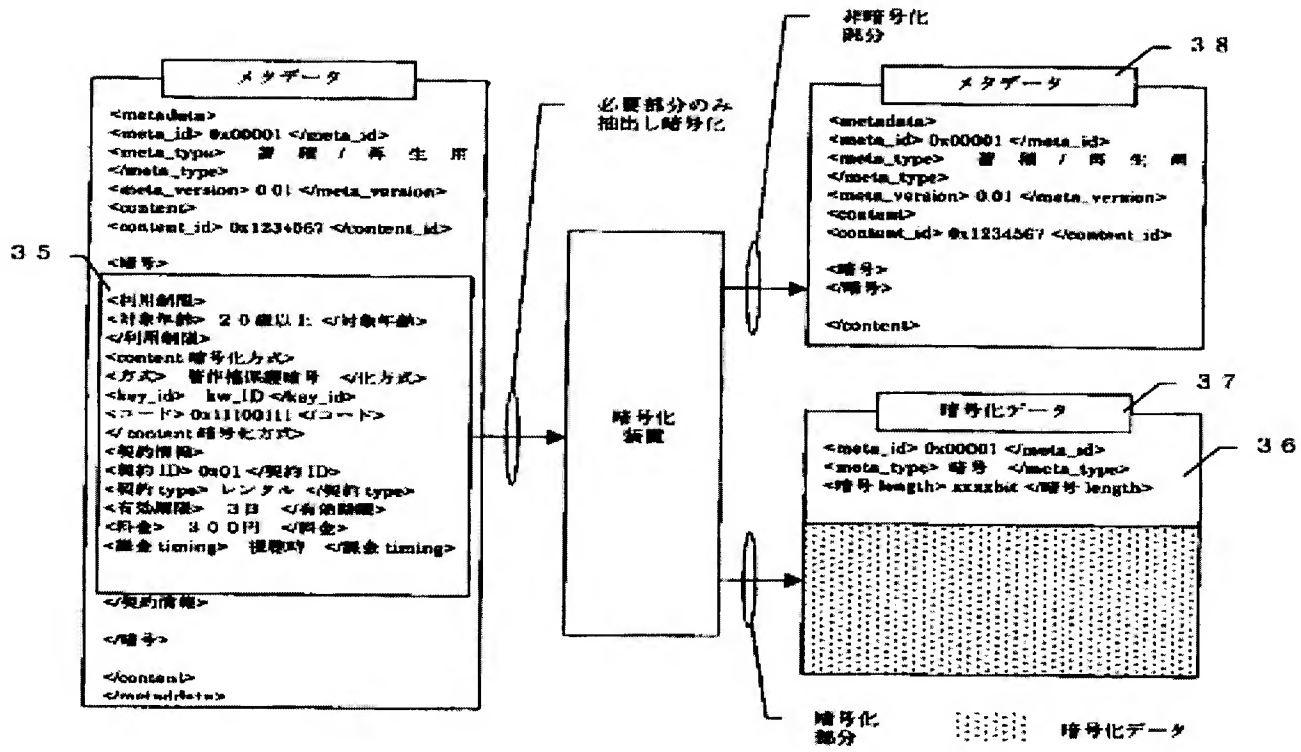
Text ...

JPEG ...

Within content, encrypted by same key

[shading] encrypted data

[Figure 6]



metadata

...
<meta_type> for storage/playback
...
<encryption>
---
35 <use restrictions>
<age target> 20 or older </age target>
</use restrictions>
<content encryption method>
<method> copyright protection encryption </conversion method>
<key_id> kw_ID </key_id>
<code> 0x11100111 </code>
</content encryption method>
<contract information>
<contract ID> 0x01 </contract ID>
<contract type> rental </contract type>
<contract term> 3 days </contract term>
<fee> 300 yen </fee>
<billing timing> when viewed </billing timing>

</contract information>

</encryption>

</content>
</metaddata [sic]>

extract and encrypt only the necessary part

encryption device

unencrypted part

metadata 38

<metadata>
...
<meta_type> for storage/playback
...
<encryption>
</encryption>

</content>

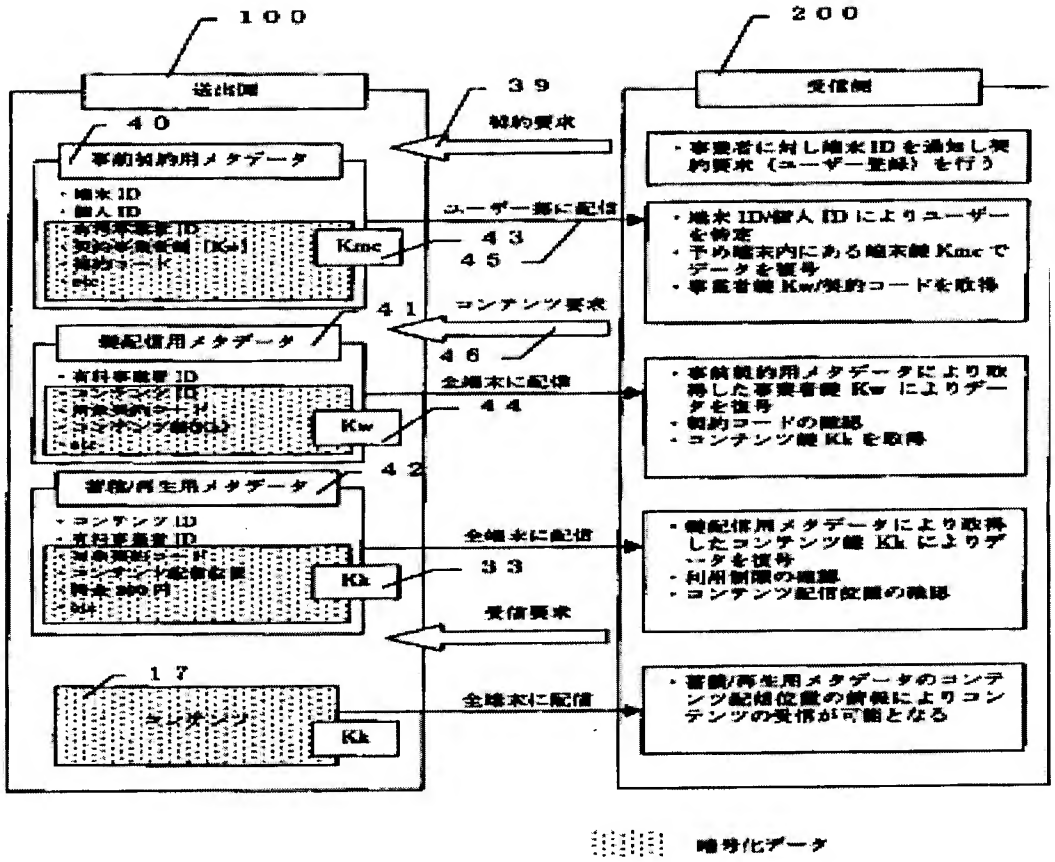
encrypted data 37

36
<meta_id> 0x00001 </meta_id>
<meta_type> encryption </meta_type>
<encryption length> xxxxbit </encryption length>

encrypted part
[shading] encrypted data

(25)

[Figure 7]



transmission side 100

metadata for prior contract 40
- terminal ID
- personal ID
- for fee business ID
- contract business key (Kw)
- contract code
- etc.

metadata for key distribution 41
- fee-charging business ID
- content ID
- relevant contract code
- content key (Kk)
- etc.

metadata for storage/playback 42
- content ID
- fee-charging business ID
- relevant contract code
- content distribution position
- fee 300 yen
- etc.

content 17

contract request 39

distribution to each user 45 →

⇐ content request 46

distribution to all terminals →

distribution to all terminals →

⇐ reception request

distribution to all terminals →

reception side 200

- notify the business of the terminal ID and make a contract request (user registration)

- specify the user by the terminal ID/personal ID
- decrypt the data with the terminal key Kmc that is previously in the terminal
- acquire the business key Kw/contract code

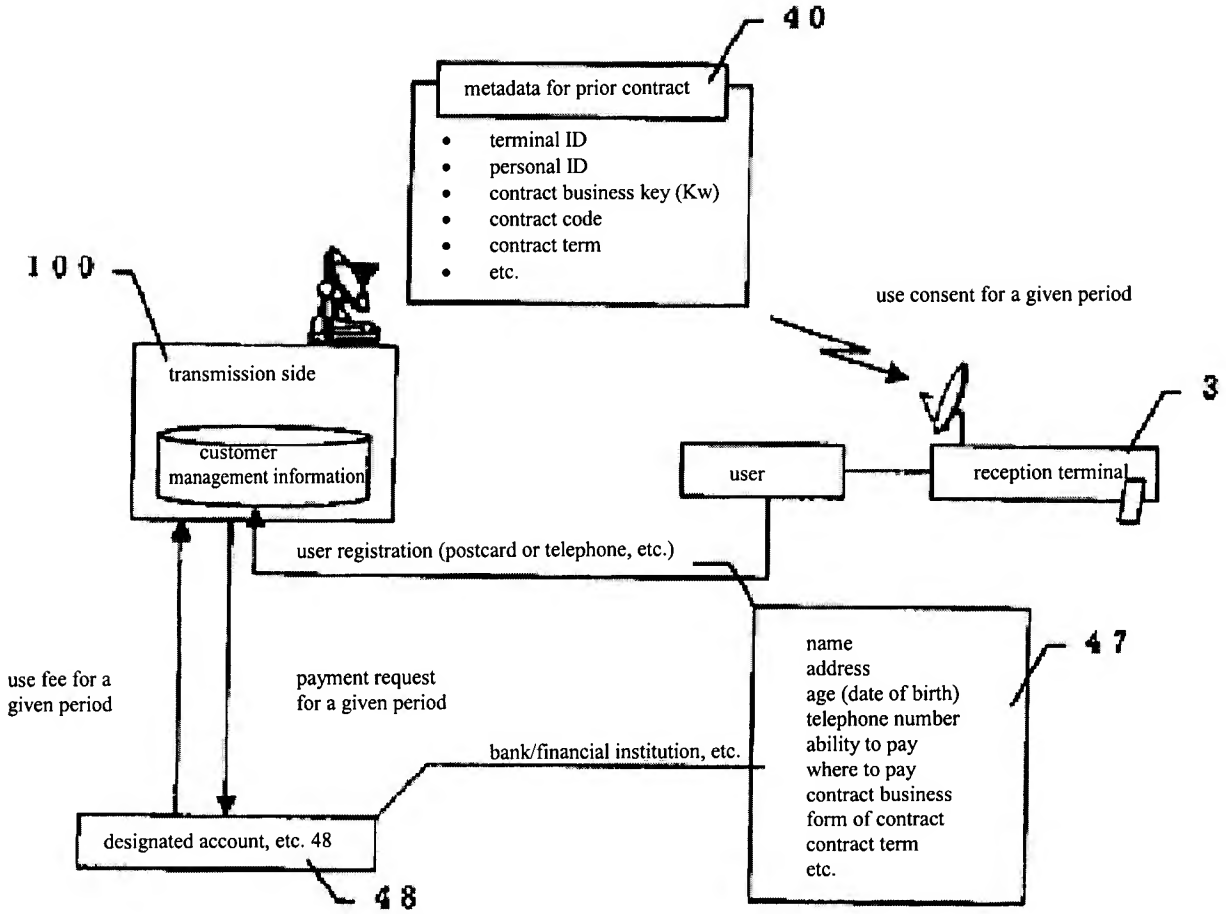
- decrypt the data with the business key Kw acquired by the metadata for prior contract
- confirm the contract code
- acquire the content key Kk

- decrypt the data with the content key Kw acquired by the metadata for key distribution
- confirmation of use restrictions
- confirmation of content distribution position

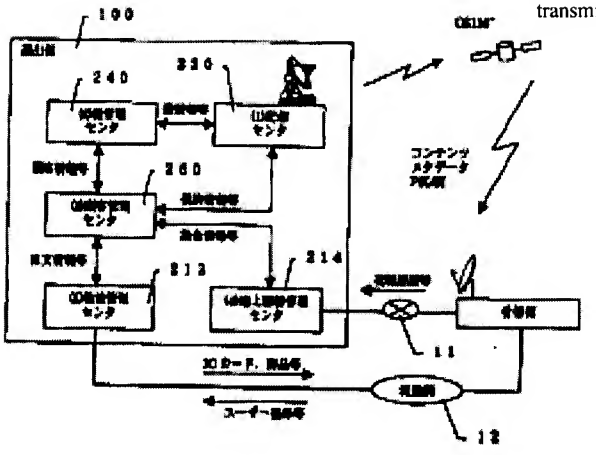
- content reception can be done by information on content distribution position in metadata for storage/playback

[shading] encrypted data

[Figure 8]



[Figure 15]



transmission side 100

key information, etc.

(2) key management center 240 ↔ (1) distribution center 220

content

contract information, etc. metadata

(3) customer mgt center 260

billing information, etc.

order information, etc.

(5) [?] mgt center 213 (4) terrestrial circuit ← viewing history, etc.

mgt center 214 reception side

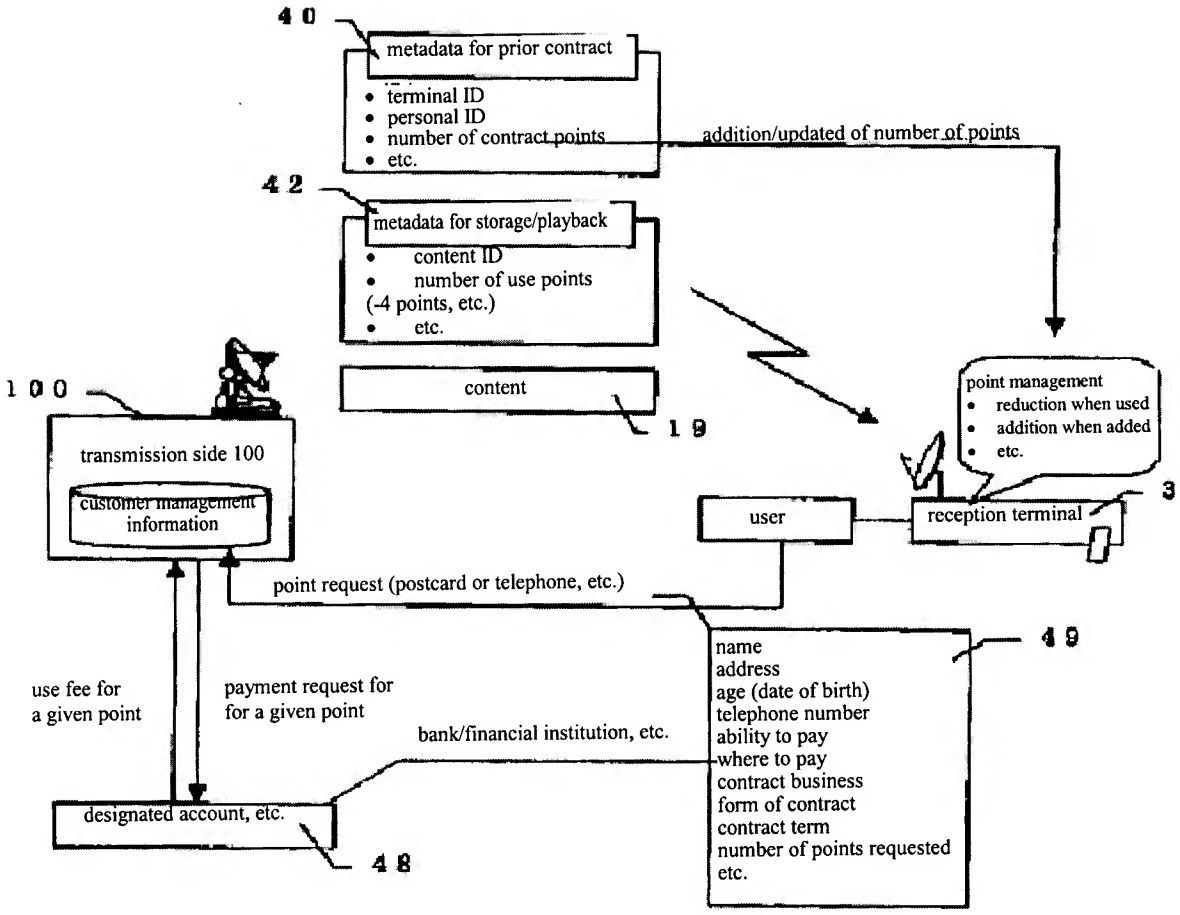
Memory card, merchandise, etc. →

[?] side 12

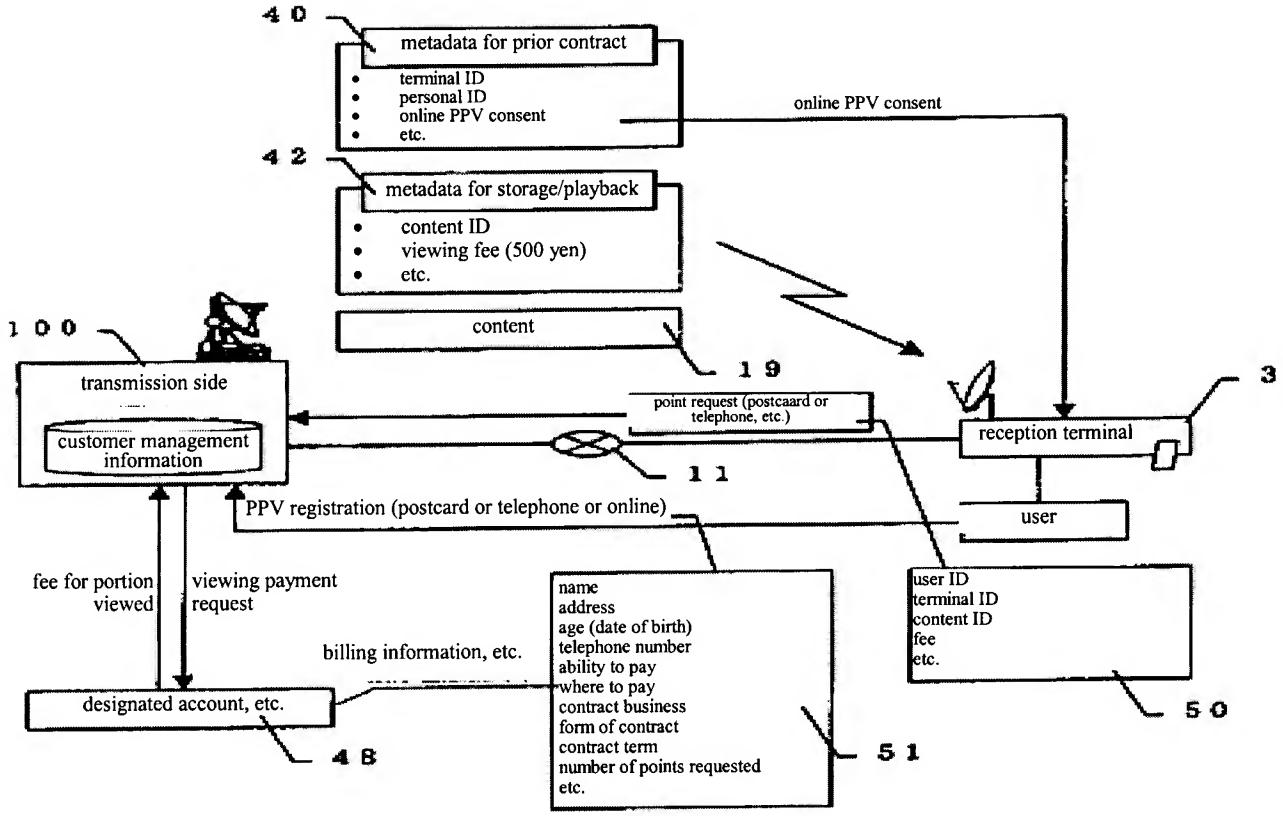
← user registration, etc.

(27)

[Figure 9]


40
metadata for prior contract
• terminal ID
• personal ID
• number of contract points
• etc.
addition/updated of number of points
42
metadata for storage/playback
• content ID
• number of use points
(-4 points, etc.)
• etc.
content
19
point management
• reduction when used
• addition when added
• etc.
100
transmission side 100
customer management information
user
reception terminal
3
point request (postcard or telephone, etc.)
49
name
address
age (date of birth)
telephone number
ability to pay
where to pay
contract business
form of contract
contract term
number of points requested
etc.
use fee for a given point
payment request for for a given point
bank/financial institution, etc.
designated account, etc.
48

[Figure 10]



[Figure 16]

[column 1:]
distribution center 220

authoring system 221
- content
- [?] file
↓
program scheduling management system 222
- content
- [?] file
↓
metadata generation device 223
customer management management center [sic] 260

[column 2:]
- program description[?] information →
- content →

- metadata →

- metadata → (for prior contract)

[column 3:]
PSI/SI generation device 224

content encryption device 225

- recording[?] position (Locator)

metadata encryption device 226

- [?] - [?]

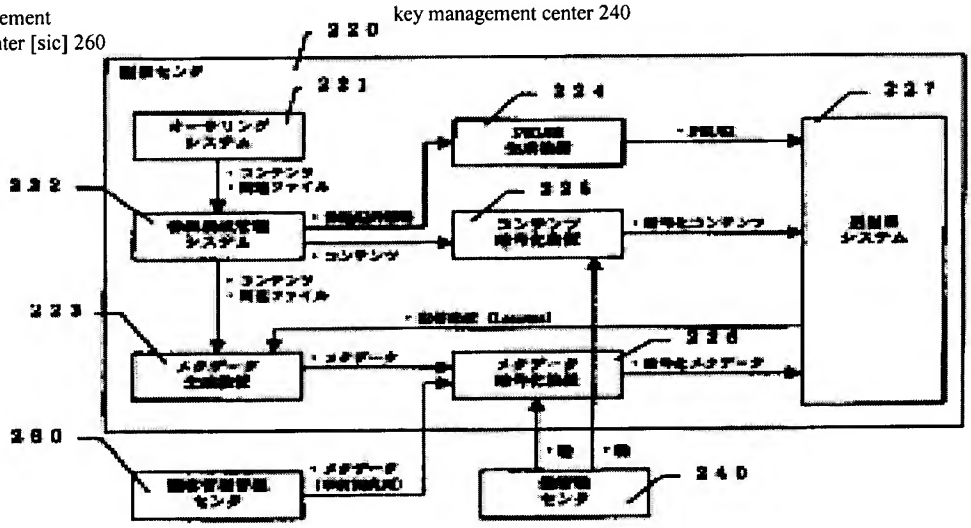
key management center 240

[column 4:]
- PSI/SI →

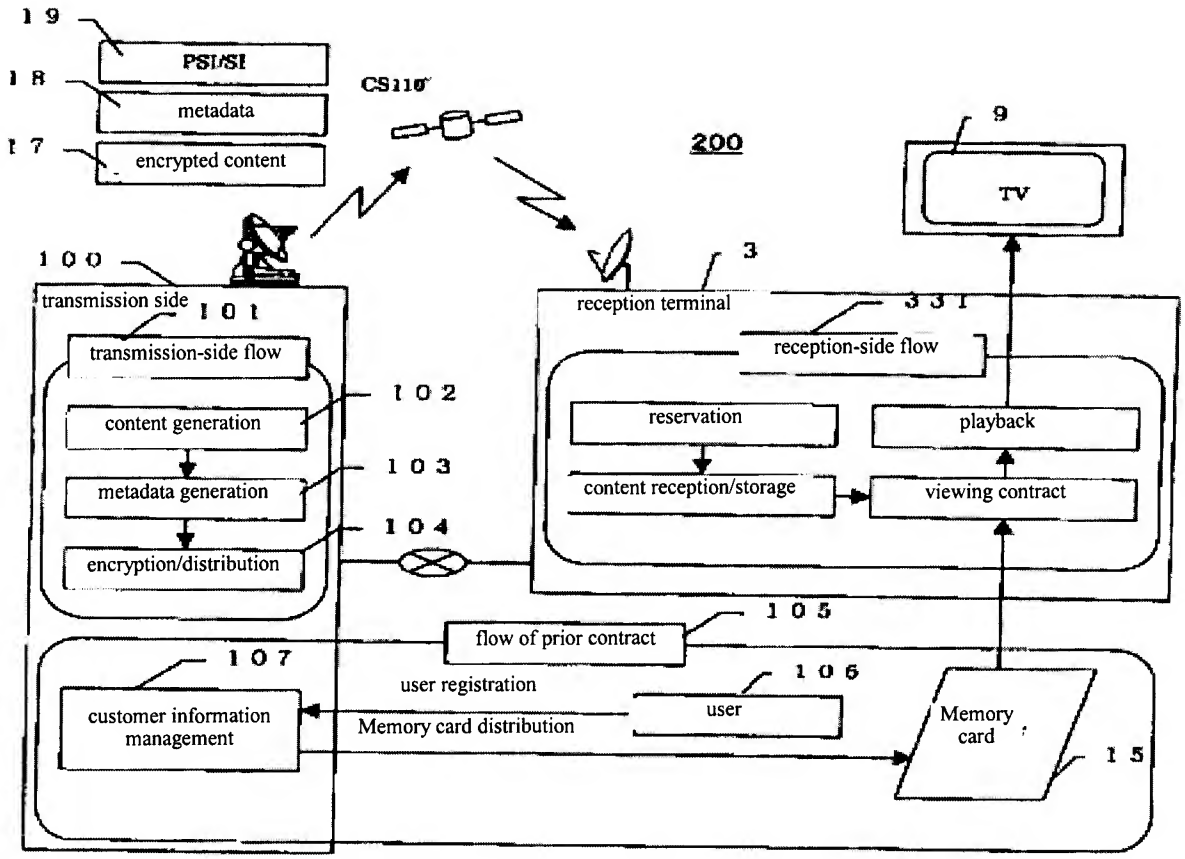
- encrypted content →

- encrypted metadata →

[column 5:]
transmission system 227



[Figure 11]



[Figure 17]

[left column:]
material 234

content title
content ID
content nature
content genre
copy control[?]
age target
producer
copyright
element composition ⇐
reference information
etc.

[middle column:]

analog input
- VHB, LD, tape, photos, etc.
digital input

authoring system

→ video authoring tools 228
→ audio authoring tools
→ data authoring tools

content management server 232
content
⇐ related[?] file 233

[right column:]

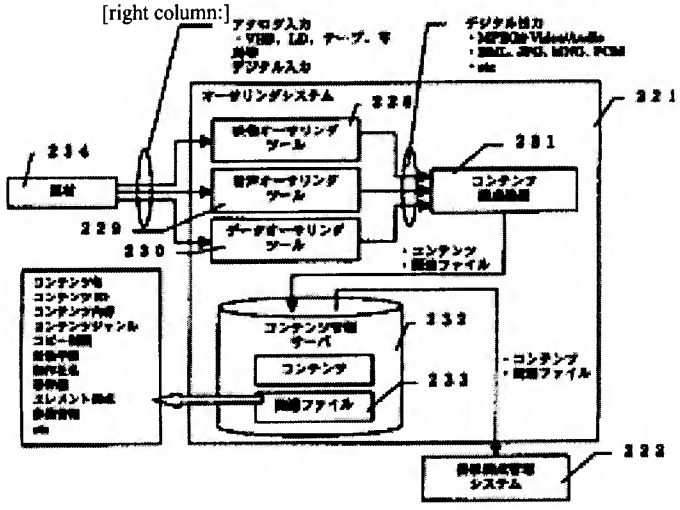
digital output
- MPEG2-Video/Audio
- BML, JPG, MNG, PCM
- etc.

content composition[?] device 231

- content
- related[?] file

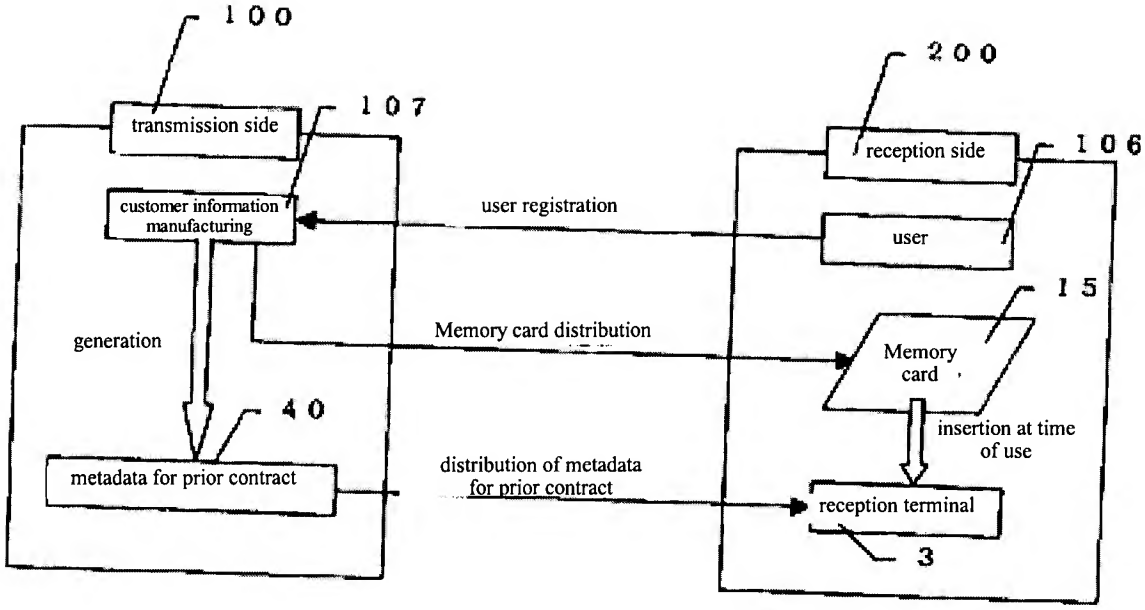
- content
- related[?] file

program scheduling management system 222



(30)

[Figure 12]



[Figure 18]

[column 1:]
program scheduling management system 222
program operation schedule generation device[?] 236
program scheduling device 235
- content
- related[?] file
content management server 232

[column 2:]
- operation schedule

- content set
- set of related files
↓ ↓
program management server 237
content 1

related files 233
⇓
program title
program ID
program nature
program genre
contract information
billing information
content composition
content [?]
etc.

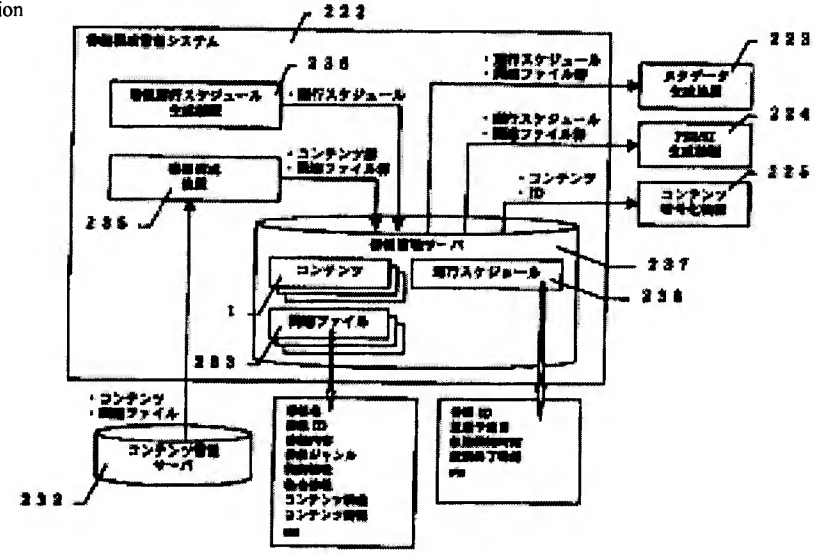
[column 3:]
- operation schedule
- set of related files

- operation schedule
- set of related files

- content
- ID

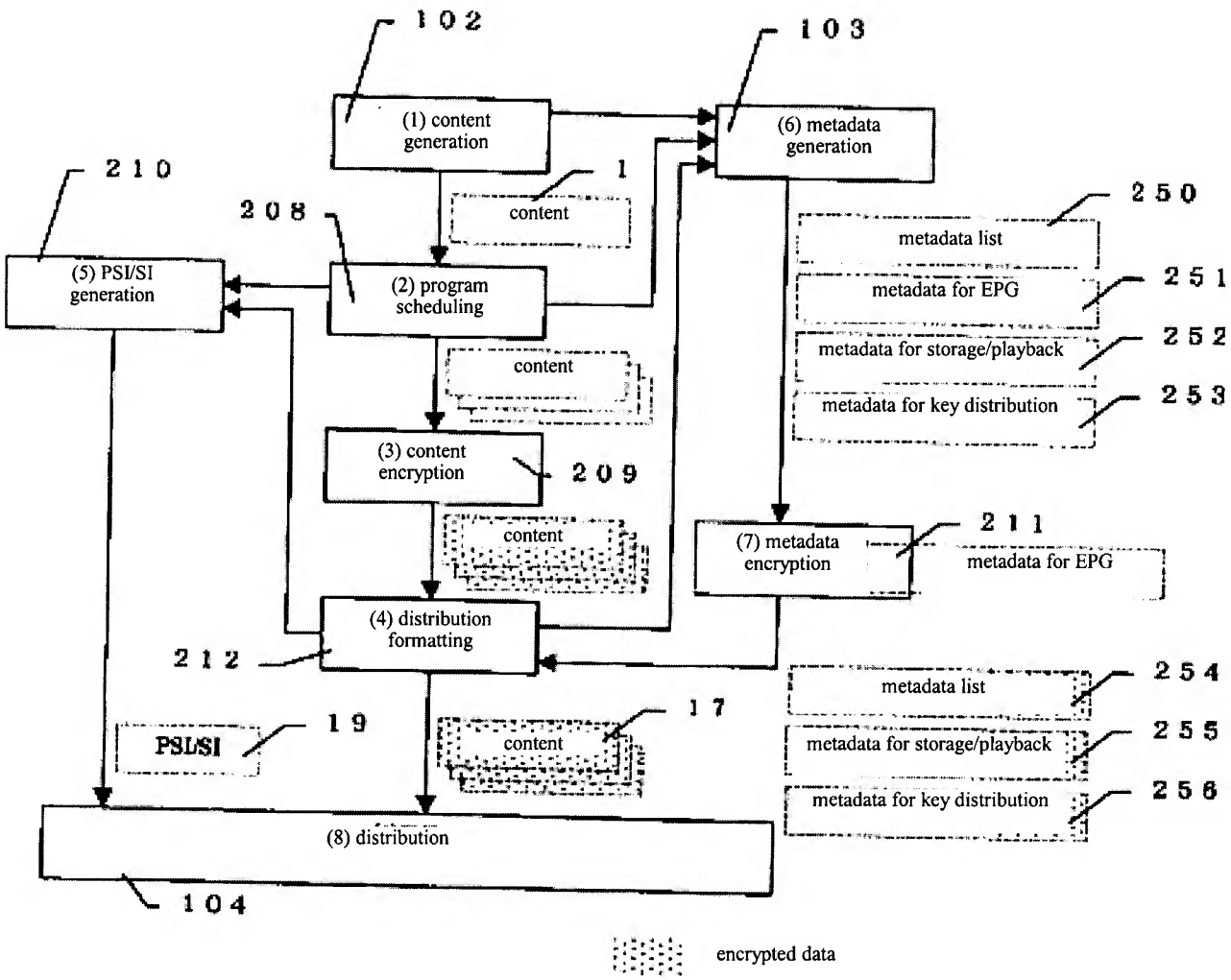
- operation schedule 238
⇓
program ID
broadcast scheduled date
broadcast starting time
broadcast ending time
etc.

[column 4:]
metadata generation device 223
PSI/SI generation device 224
content encryption device 225



(31)

[Figure 13]


102
103
(1) content generation
(6) metadata generation
210
1
content
208
250
metadata list
(5) PSI/SI generation
(2) program scheduling
metadata for EPG
251
metadata for storage/playback
252
content
metadata for key distribution
253
(3) content encryption
209
content
211
(7) metadata encryption
metadata for EPG
(4) distribution formatting
212
metadata list
254
17
19
PSI/SI
content
metadata for storage/playback
255
metadata for key distribution
256
(8) distribution
104
encrypted data

(32)

[Figure 20]

[column 1:]
program scheduling management system 222
program management server 237

[column 2:]
- content ID

- set of related files
- operation schedule

metadata for EPG 251
- program ID
- content ID
- content composition
- etc.

metadata list 250
- content ID
- metadata ID
- metadata distribution position
- etc.

[column 3:]
key management center 240

metadata generation device 223

[column 4:]
- content key (Kk)

- content distribution position
- metadata distribution position

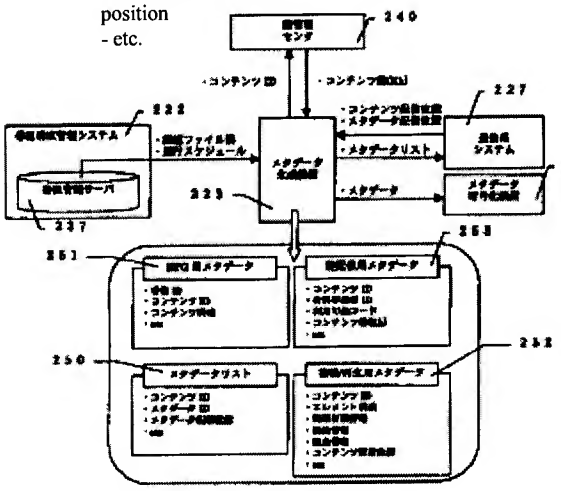
- metadata list

- metadata

metadata for key distribution 253
- content ID
- fee-charging business ID
- usable[?] code
- content key (Kk)
- etc.

metadata for storage/playback 252
- content ID
- element composition
- use [?] information
- contract information
- billing information
- content distribution position
- etc.

[column 5:]
transmission system 227
metadata encryption device 226



[Figure 21]

[column 1:]
program scheduling management system 222
program management server 237

[column 2:]
- content ID

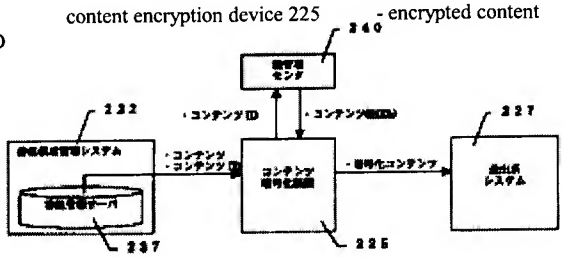
- content
- content ID

[column 3:]
key management center 240
↑↓
content encryption device 225

[column 4:]
- content key (Kk)

- encrypted content

[column 5:]
transmission system 227



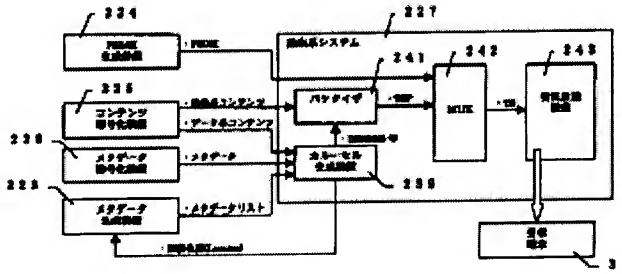
[Figure 23]

[column 1:]
PSI/SI generation device 224
content encryption device 225
metadata encryption device 226
metadata generation device 223

[column 2:]
- PSI/SI
- image content
- data content
- metadata
- metadata list
- distribution position (Locator)

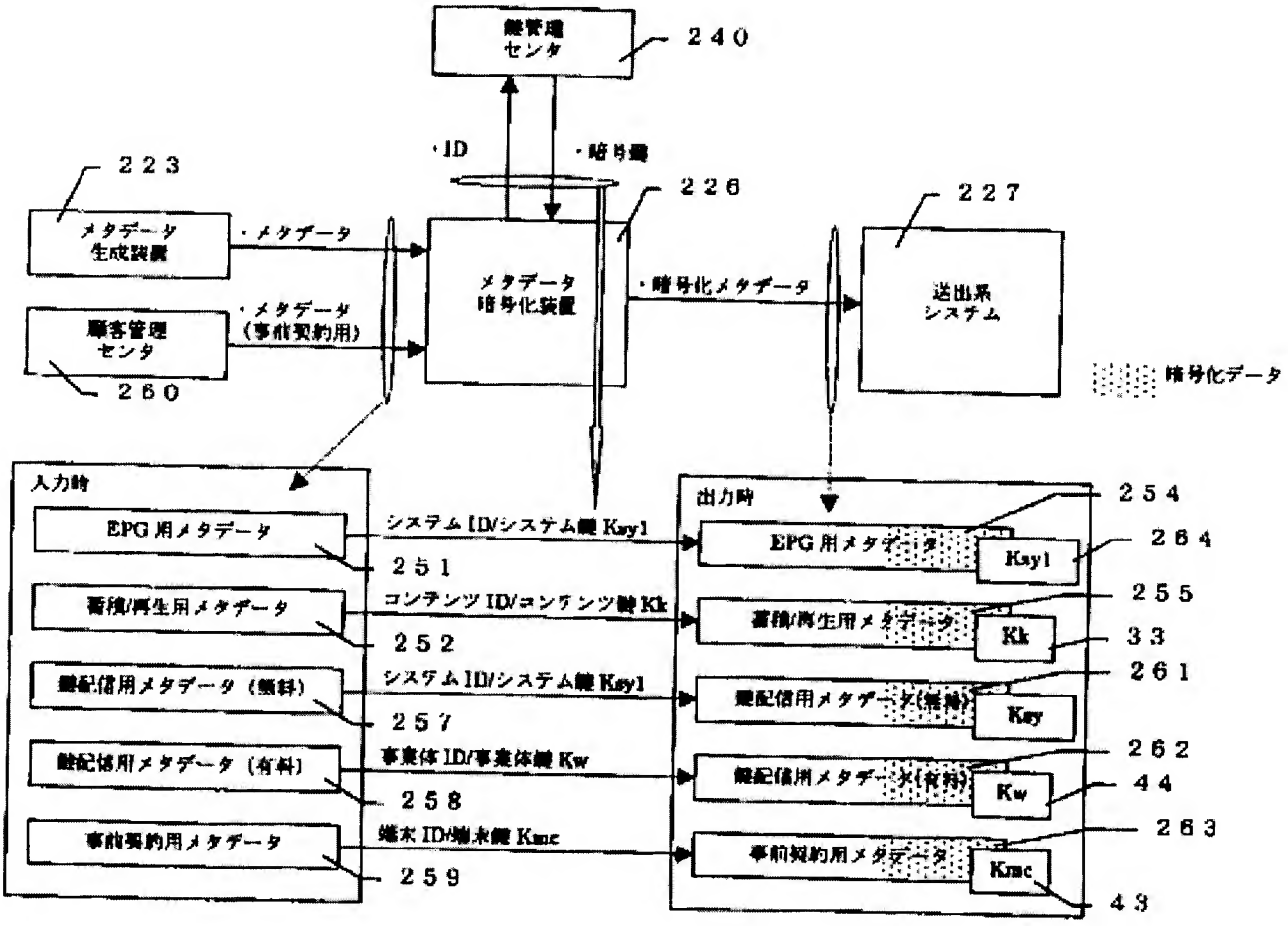
[column 3:]
transmission system 227
packetizer 241
↑ DII/DDB, etc.
carrousel generation device 239

[column 4:]
entrusted broadcasting equipment 243
reception terminal 3



(33)

[Figure 22]



metadata generation device 223
- metadata →

customer management center 260
- metadata (for prior contract) →

Upon input
metadata for EPG 251
metadata for storage/playback 252
metadata for key distribution (free) 257
metadata for key distribution (for fee) 258
metadata for prior contract 259

key management center 240
- ID ↑↓ - encryption key
metadata encryption device 226
- encryption metadata →

system ID/system key Ksy1
content ID/content key Kk
system ID/system key Ksy1
business body ID/business body key Kw
terminal ID/terminal key Kmc

transmission system
[shading] encrypted data

Upon output
metadata for EPG 254
metadata for storage/playback 255
metadata for key distribution (free) 261
metadata for key distribution (for fee) 262
metadata for prior contract 263

[Figure 24]

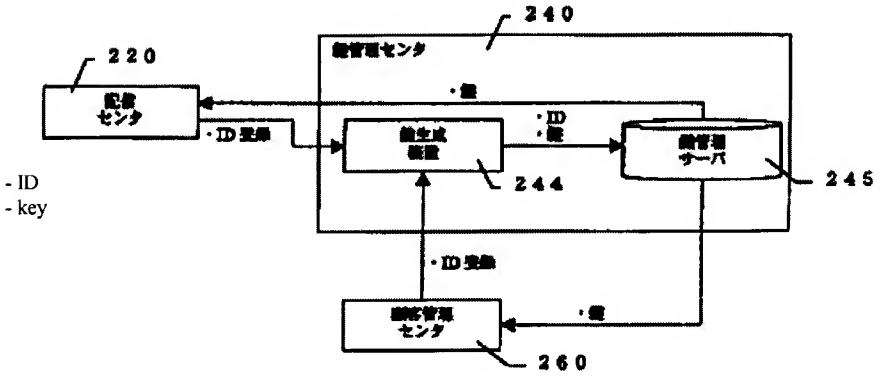
[left column:]
distribution center 220
- ID registration

[middle column:]
key management center 240
- key

key generation device 244

- ID registration
customer management center 260

[right column:]
key management server 245



[Figure 25]

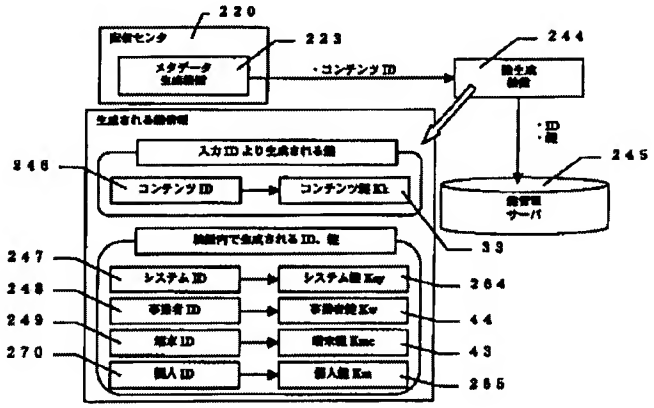
distribution center 220
metadata generation device 223 - content ID

generated key information
- ID
key generated by input ID - key
content ID 246 → content key Kk

ID, key generated within device
system ID 247 system key Key 264
business ID 248 business key Kw 44
terminal ID 249 terminal key Kmc 43
personal ID 270 personal key Km 255

key generation device 244

key management server 245



[Figure 26]

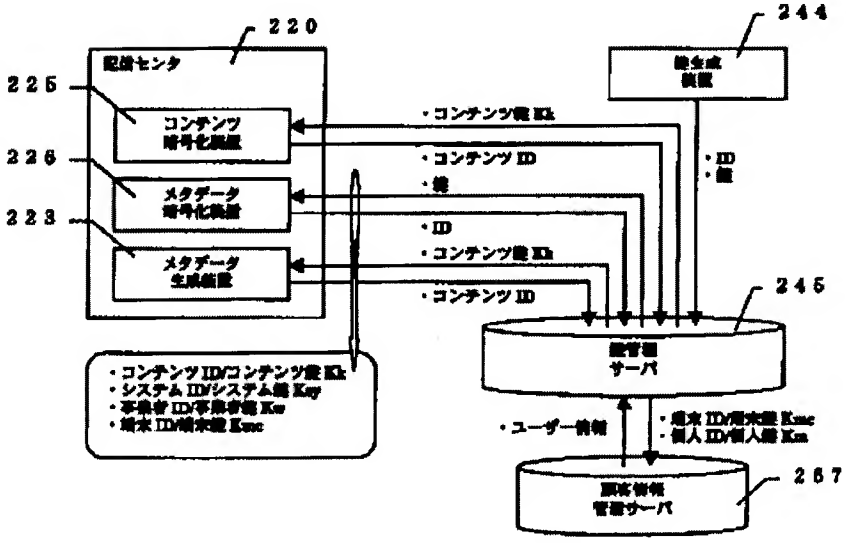
[left column:]
distribution center 220
content encryption device 225
metadata encryption device 226
metadata generation device 223

- content ID/content key Kk
- content ID/system key Ksy
- business ID/business key Kw
- terminal ID/terminal key Kmc

[middle column:]
- content key Kk
- content ID
- key
- ID
- content key Kk
- content ID

- user information

[right column:]
key generation device 244
- ID
- key
key management server 245
- terminal ID/terminal key Kmc
- personal ID/personal key Km
↑↓
customer information manufacturing server 267

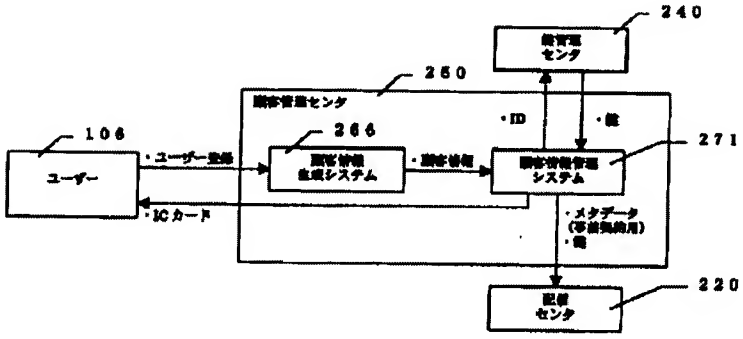


[Figure 27]

[left column]
- user registration
user 106
- Memory card

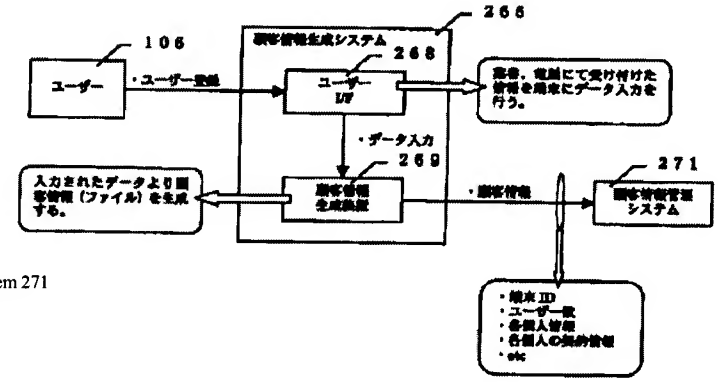
[middle column:]
customer management center 260
customer information generation system 266 - customer information →

[right column:]
key management center 240
- ID - key
customer information management system 271
- metadata (for prior contract)
- key[?]
distribution center 220



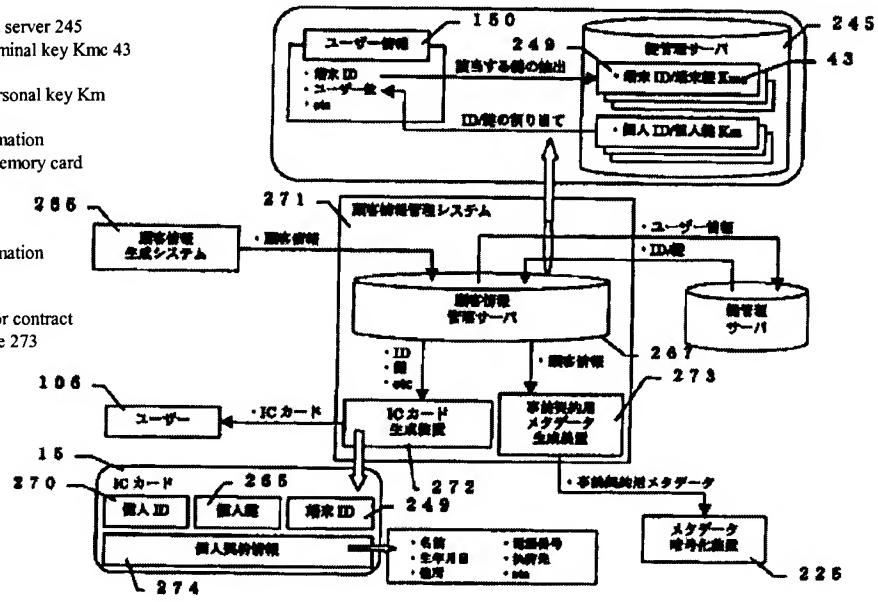
[Figure 28]

[left column:]
- user registration →
user 106
Customer information (file) is generated according to the data that is input.
[middle column:]
customer information generation system 266
user I/F
- data input
customer information generation device 269
[right column:]
Information received by postcard or telephone is data-input into the terminal.
- customer information → customer information management system 271
- terminal ID
- number of users
- personal information on each individual
- contract information on each individual
- etc.

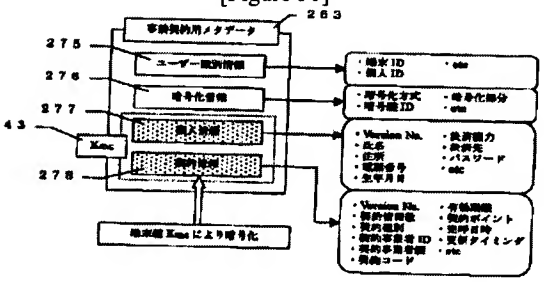


[Figure 29]

[round-cornered rectangle at top:]
user information 150
- terminal ID extract relevant key → - terminal ID/terminal key Kmc 43
- number of users
- etc. assign an ID/key - personal ID/personal key Km
[items at left:]
customer information generation system 266 - customer information
user 106 ← - Memory card
[large square in middle:]
customer information management system 271
customer information management server 267
- ID ↓ ↓ - customer information
- key
- etc.
Memory card metadata for prior contract
generation device 272 generation device 273
[to right of big square in middle:]
- user information
- ID/key
key management server
15 – memory card
270 – personal ID
265 – personal key
249 – terminal ID
274 – personal contract information
[rectangle at middle bottom:]
- name - telephone number
- date of birth - where to pay
- address - etc.
[items in lower right:]
- metadata for prior contract
metadata encryption device 226



[Figure 30]



[left column:]
metadata for prior contract 263
user identification information 275
encryption information 276
personal information 277
contract information 278
⇑
encryption by terminal key Kmc

[right column:]
- terminal ID
- personal ID
- etc.

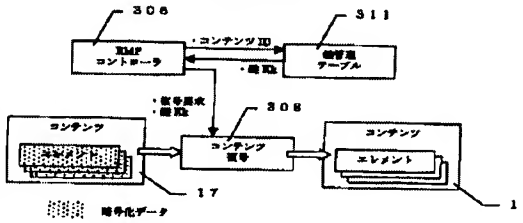
- encryption method
- encryption key ID
- encrypted part
- etc.

- Version No.
- name
- address
- telephone number
- date of birth
- ability to pay
- where to pay
- password
- etc.

- Version No.
- contract information number
- contract type
- contract business ID
- contract business key
- contract code
- effective term
- contract points
- [illegible] purpose
- update timing
- etc.

[shading] encrypted data

[Figure 38]



RMP controller 306 — content ID → / ← key Kk — key management table 311

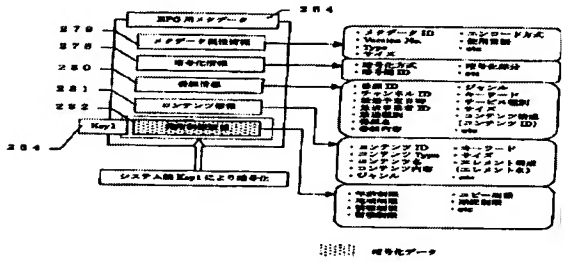
- decryption request
- key Kk

content 17 — content 1

elements ⇒ content decryption 308 — elements

[shading] encrypted data

[Figure 31]

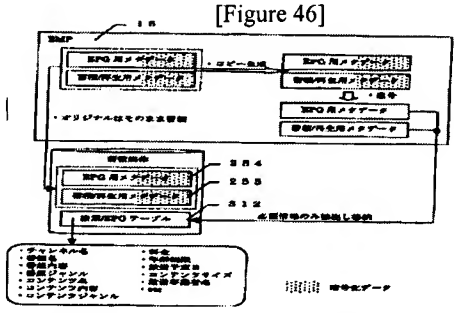


[left column:]
metadata for EPG 254
metadata attribute information 279
encryption information 276
program information 280
content information 281
use restrictions information 282
⇑
encryption by system key Ksy1

[right column:]
- metadata ID
- Version No.
- Type
- size
- encryption method
- encryption key ID
- program ID
- channel ID
- scheduled broadcast time
- broadcaster ID
- type of broadcast
- program title
- program nature
- content ID
- content Type
- content title
- content nature
- genre
- age restrictions
- region restrictions
- viewing restrictions
- storage restrictions
- encoding method
- language used
- etc.
- encrypted part
- etc.
- genre
- password
- type of service
- size
- content composition (content ID)
- etc.
- keyword
- size
- element composition (element title)
- etc.
- copy restrictions
- time restrictions
- etc.

[shading] encrypted data

[Figure 46]



[left column:]
metadata for EPG
- copy generation
metadata for storage/playback

- original stored[?] as is

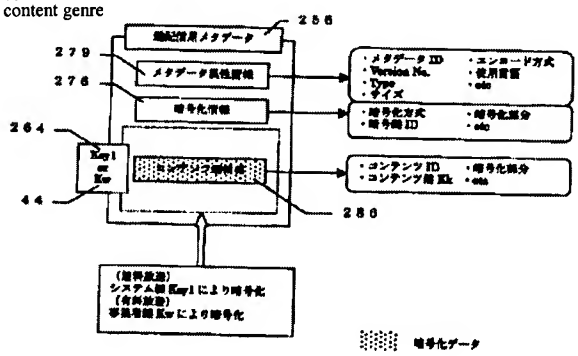
storage medium
metadata for EPG 254
metadata for storage/playback 255
retrieval/EPG table 312
↓
- channel name
- program title
- program nature
- program genre
- content title
- content nature
- content genre
- fee
- age restrictions
- scheduled broadcast time
- content size
- broadcaster name
- etc.

[right column:]
metadata for EPG
metadata for storage/playback
⇓ - decryption
metadata for EPG
metadata for storage/playback

extract and store necessary information only

[shading] encrypted data

[Figure 33]



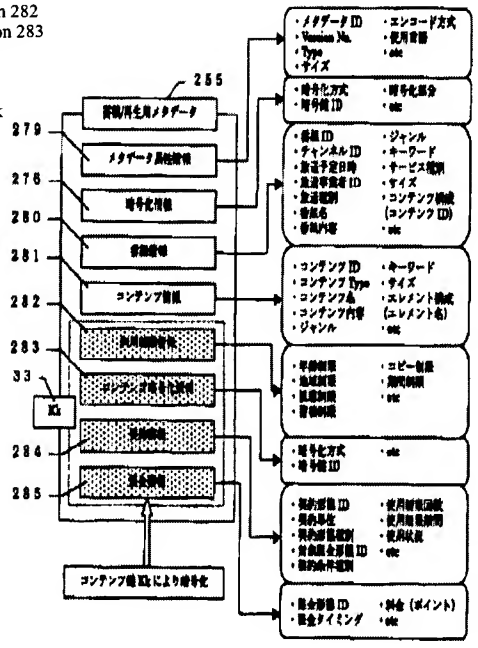
[left column:]
metadata for key distribution 256
metadata attribute information 279
encryption information 276
content key information 286
⇑
(free broadcast)
encryption by system key Ksy1
(for-fee broadcast)
encryption by business key Kw

[right column:]
- metadata ID
- Version No.
- Type
- size
- encryption method
- encryption key ID
- content ID
- content key Kk
- encoding method
- language used
- etc.
- encrypted part
- etc.
- encrypted part
- etc.

[shading] encrypted data

[Figure 32]

[left column:]
metadata for storage/playback 255
metadata attribute information 279
encryption information 276
program information 280
content information 281
use restrictions[?] information 282
content encryption information 283
contract[?] information 284
billing[?] information[?] 285
⇑
encryption by content key Kk



[right column:]
- metadata ID — encoding method
- Version No. — language used
- Type — etc.
- size

- encryption method — encrypted part
- encryption key ID — etc.

- program ID — genre
- channel ID — password
- scheduled broadcast time — type of service
- broadcaster ID — size
- type of broadcast — content composition (content ID)
- program title
- program nature — etc.

- content ID — keyword
- content Type — size
- content title — element composition (element title)
- content nature
- genre — etc.

- age restrictions — copy restrictions
- region restrictions — time restrictions
- viewing restrictions — etc.
- storage restrictions

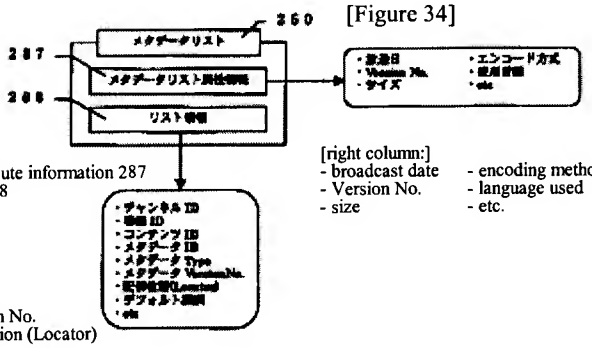
- encryption method — etc.
- encryption key ID

- contract form ID — restricted number of uses
- contract unit — use restrictions period
- contract form type — state of use
- billing form ID — etc.
- contract conditions type

- billing form ID — fee (points)
- billing timing — etc.

[shading] encrypted data

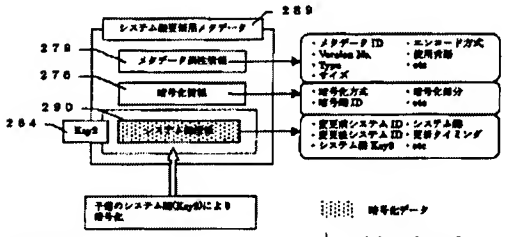
[Figure 34]



[left column:]
metadata list 250
metadata list attribute information 287
list information 288
↓
- channel ID
- program ID
- content ID
- metadata ID
- metadata Type
- metadata Version No.
- distribution position (Locator)
- default type[?]
- etc.

[right column:]
- broadcast date — encoding method
- Version No. — language used
- size — etc.

[Figure 35]

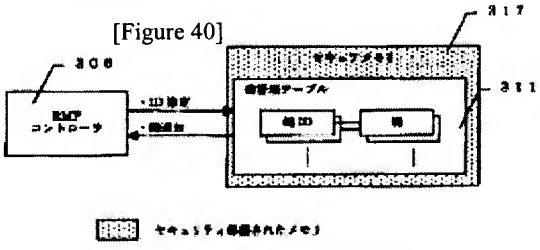


[Figure 35]
[left column:]
metadata for system key updating 289
metadata attribute information 279
encryption information 276
system key information 290
⇑
encryption by spare system key (Key2)

- [right column:]
- metadata ID — encoding method
- Version No. — language used
- Type — etc.
- size
- encryption method — encrypted part
- encryption key ID — etc.
- pre-change system ID — system key
- post-change system ID — update timing
- system key Key3 — etc.

[shading] encrypted data

[Figure 40]



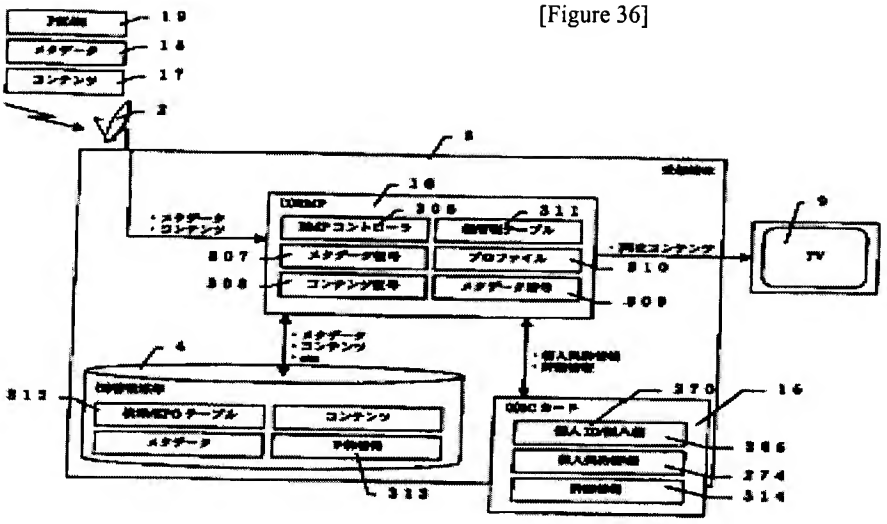
secure memory 317
key management table
- ID designation →
RMP controller 306 ← - key notification
key ID — key[?] 311

[shading] security-protected memory

[Figure 50]

Content type	Element
Image content	- MPEG2-Video stream (PES) - MPEG2-Audio stream (PES) - MPEG1-Video stream (PES) - other
Data content	- EML - XML - Text - JPG - MWG - MPEG2-Video - MPEG2-Audio - MPEG1-Video - MPEG1-PS - MPEG2-PS - Other

[Figure 36]



[column 1:]
PSI/SI 19
metadata 18
content 17

[column 2:]
- metadata
- content

(2) storage medium
retrieval/EPG table 312
metadata

[column 3:]
(1) RMP
RMP controller 306
metadata decryption 307
content decryption 308
↑
- metadata
- content
- etc.

content
reservation information 313

[column 4:]
key management table 311
profile 310
metadata encryption 309

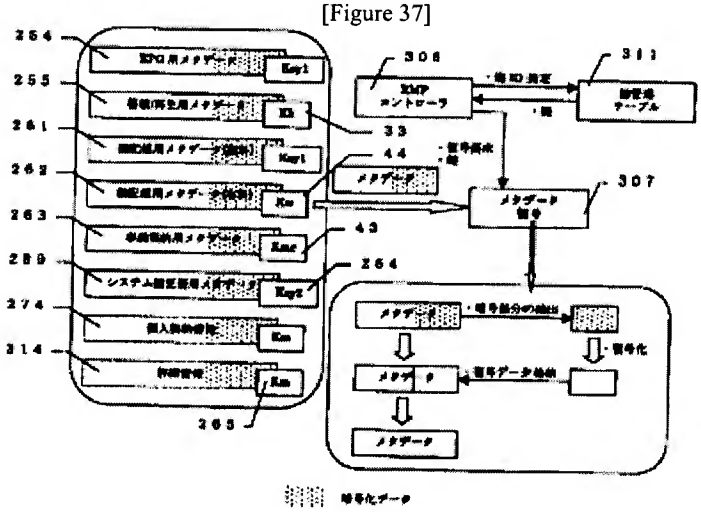
[column 5:]
reception terminal

- playback content →

- personal contract information
- consent[?] information

(3) Memory card
personal ID/personal key[?] 265
personal contract information 274
consent[?] information 314

[Figure 37]



[column 1:]
metadata for EPG 254
metadata for storage/playback 255
metadata for key distribution (free) 261
metadata for key distribution(for fee) 262
metadata for prior contract 263
metadata for system key updating 289
personal contract information 274
consent information 314

[column 2:]
RMP controller 306
- decryption request
- key

metadata
⇒
metadata
⇓
metadata
⇓
metadata

[shading] encrypted data

[column 3:]
key ID designation

- key

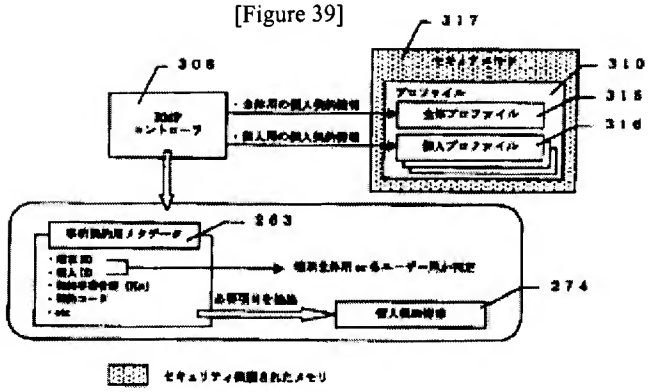
metadata decryption 307
⇓
- extraction of encrypted part
- storage of decryption data

[column 4:]
key management table 311

⇓ - decryption

(39)

[Figure 39]



secure memory 317
profile 310
overall profile 315
personal profile 316

RMP controller 306
⇓
- personal contract information for all →
- personal contract information for individual →

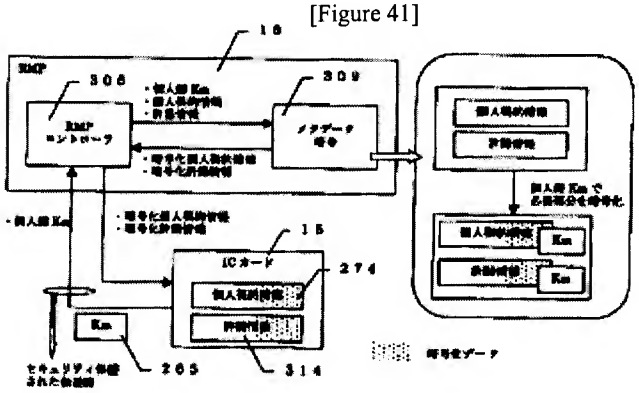
metadata for prior contract 263
- terminal ID
- personal ID
- contract business key (Kw)
- contract code
- etc.

→ decide whether for all terminals or for each user

extract necessary items
⇒ personal contract information 274

[shading] security-protected memory

[Figure 41]



[column 1:]
RMP
RMP controller 306
- personal key Kmc
⇓
security-protected transmission channel

[column 2:]
- personal key Km
- personal contract information
- consent information

- encrypted personal contract information
- encrypted consent information

- encrypted personal contract information
- encrypted consent information

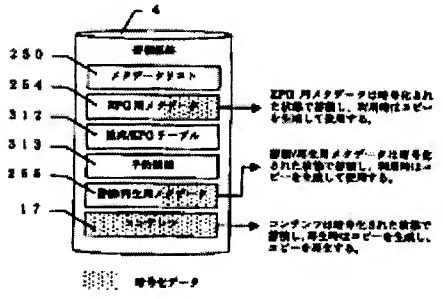
[column 3:]
metadata encryption 309

Memory card 15
personal contract information 274
consent information 314

[column 4:]
personal contract information
consent information
↓ encryption of necessary part by personal key Km
personal contract information
consent information

[shading] encrypted data

[Figure 42]



[column 1:]
storage medium
metadata list 250
metadata for EPG 254
retrieval/EPG table 312
reservation information 313
metadata for storage/playback 255
content 17

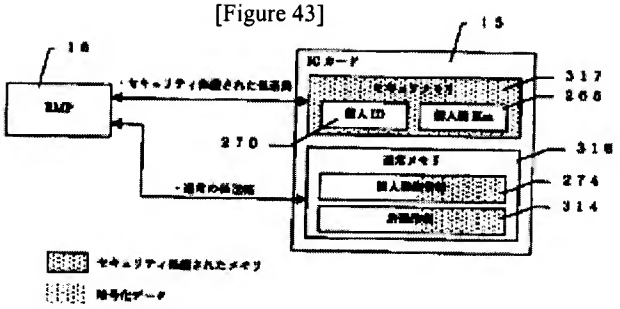
[shading] encrypted data

[column 2:]
→ The metadata for the EPG is stored in encrypted form, and when used, a copy is generated and used.

→ The metadata for storage/playback is stored in encrypted form, and when used, a copy is generated and used.

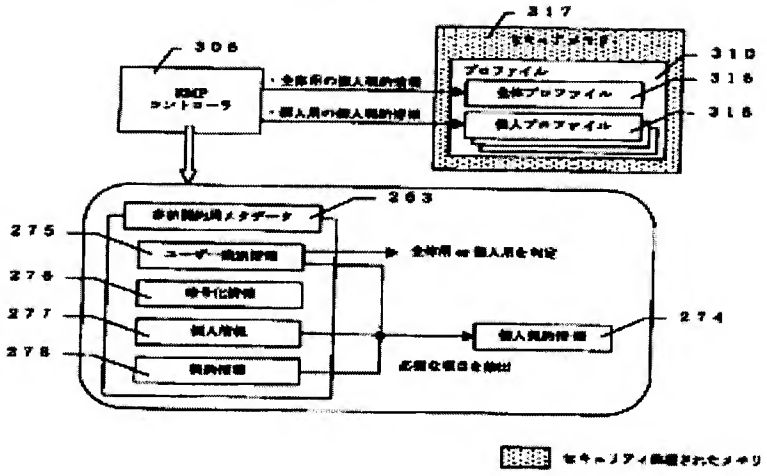
→ The content is stored in encrypted form, and when played back, a copy is generated and the copy is played back.

[Figure 43]



Memory card 15
- security-protected transmission channel
RMP 16
personal ID 270
secure memory 317
personal key Km 265
ordinary memory 318
- ordinary transmission channel
personal contract information 274
consent information 314
[shading] security-protected memory
[shading] encrypted data

[Figure 44]



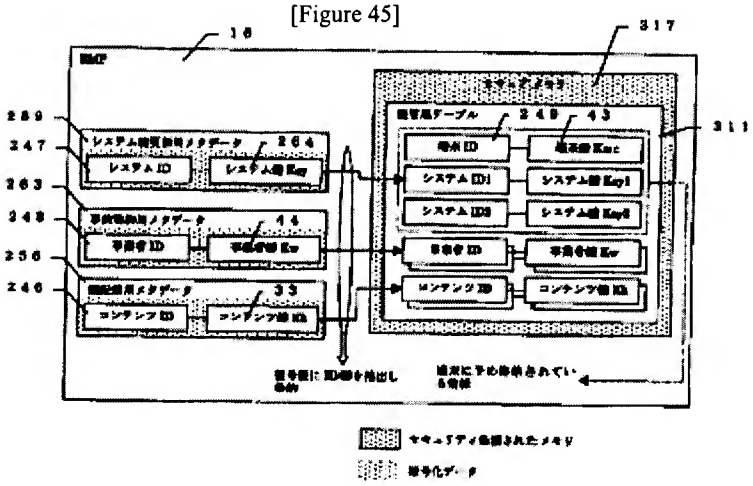
secure memory 317
profile 310
RMP controller 306
- personal contract information for all
- personal contract information for an individual
overall profile 315
personal profile 316
⇓
metadata for prior contract 263
user identification information 275
→ decide whether for all or for an individual
encryption information 276
personal information 277
→ individual contract information 274
contract information 278
extract necessary items
[shaded] security-protected memory

[Figure 51]

Data type	Encryption key type	Supplementary
content	content key (Kk)	key unique to content
metadata list	none	encryption not done
metadata for prior contract	terminal key (Kmc)	key unique to each terminal
metadata for EPG	system key (Ksy1)	key in common for whole system
metadata for storage/playback	content key (Kk)	key unique to each content
metadata for key distribution (free)	system key (Ksy1)	key on common for whole system
metadata for key distribution (for fee)	business key (Ky)	key unique to each business
metadata for system key updating	system key (Ksy2)	key in common for whole system (spare)

(41)

[Figure 45]



[column 1:]
RMP
metadata for system key updating 289
system ID 247
metadata for prior contract 263
business ID 248
metadata for key distribution 256
content ID 246

[column 2:]
system key Ksy 264
business key Kw 44
content key Kk 33
extract and store ID/key after decryption

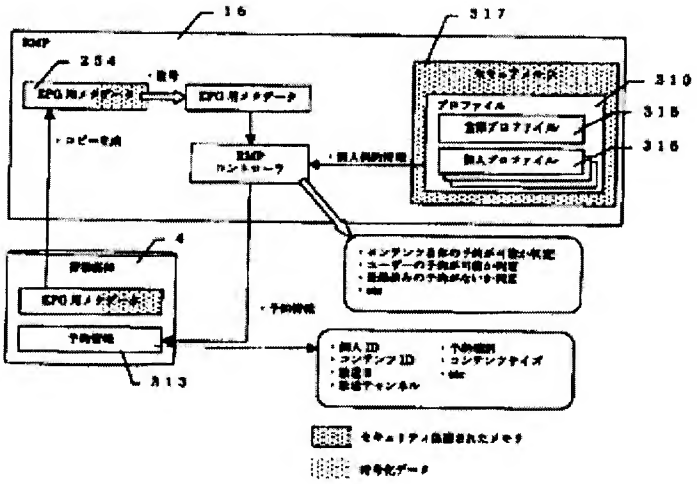
[column 3:]
secure memory 317
key management table
terminal ID
system ID1
system ID2
business ID
content ID

information pre-stored in terminal ←

[shading] security-protected memory
[shading] encrypted data

[column 4:]
terminal key Kmc
system key Ksy1
system key Ksy2
business key Kw
content key Kk

[Figure 47]



[column 1:]
RMP
- decryption
metadata for EPG 254
- copy generation
storage medium 4
metadata for EPG
reservation information 313

[column 2:]
metadata for EPG
RMP controller

[column 3:]
- personal contract information

- decide whether content itself can be reserved
- decide whether use reservation is possible
- decided whether there is no recorded reservation
- etc.

- reservation information

- personal ID
- content ID
- broadcast date
- broadcast channel
- reservation type
- content size
- etc.

[shading] security-protected memory
[shading] encrypted data

[column 4:]
secure memory
profile 310
overall profile 315
personal profile 316

[Figure 48]

[left column:]
RMP
RMP controller
- personal ID
- personal key
Memory card
secure memory 317
personal ID 270 personal key Km 266
ordinary memory 318
personal contract information
consent information
⇓
- version No. - contract business ID
- [?] - [?] of contract information
- [?] - contract type
- [?] - contract [?]
- address - contract [?]
- [?] - [?]
- [?] - [?]

[middle column:]
- extract relevant personal contract information
- personal key/personal contract information

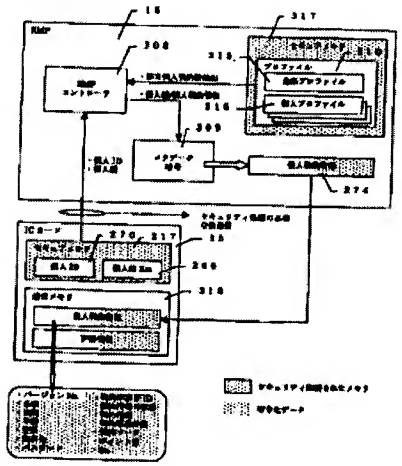
metadata decryption 309

→ transmission channel requiring security protection

[right column:]
secure memory 317
profile 310
overall profile 315
personal profile 316

personal contract information[?] 274

[shading] security-protected memory
[shading] encrypted data



[Figure 49]

[column 1:]
RMP
- decryption metadata for storage/playback
- copy generation storage medium 4
metadata for storage/playback 255

[column 2:]

metadata for storage/playback
↓
RMP controller 306
- personal key
- personal contract information

Memory card 5
secure memory 317
personal ID 270 personal key Km 265

ordinary memory
personal contract information 274
consent information
⇓
- content ID - [?]
- content title - [?]
- genre - [?]
- [?] - [?]
- [?] - [?]

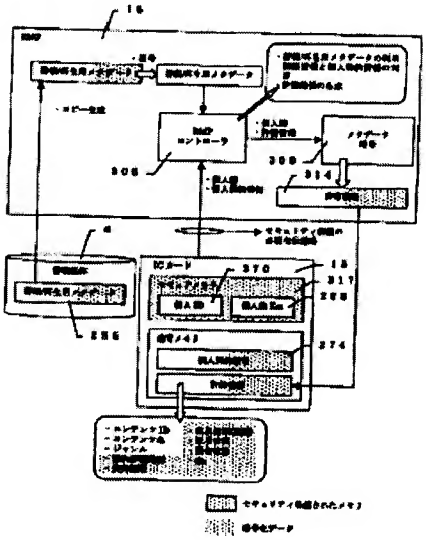
[shading] security-protected memory
[shading] encrypted data

[column 3:]
- decision of use restriction information and personal contract information of metadata for storage/playback
- generation of consent information

- personal key
- consent information

metadata encryption 309
⇓
consent information 314

→ transmission channel requiring security protection



[Figure 52]

Main functions of RMP controller

Function	Description
Reception control	- Function that decides by metadata for storage/playback, metadata for key distribution, and profile whether it is content that can be received, and controls reception of the content
Storage control	- Function that controls by the metadata for the EPG, metadata for storage/playback, the metadata list, etc. the operation of storing in a storage medium the content, metadata, etc. that is generated within RMP
Copy control	- Function that controls, by the metadata for storage/playback, copy requests to removable media, etc. that are generated by a user request, etc. such as a viewing contract
Presentation control	- Function that controls, in response to a user viewing request, the playback of content based on information in metadata for storage/playback and consent information generated by a viewing contract
Viewing contract control	- Function that generates consent information with respect to content viewing based on metadata for storage/playback and personal contract information within an memory card
Billing control	- Function that controls billing processing done based on point information, etc stored in the metadata for storage/playback and personal contract information within an memory card
Personal authentication control	- Function that controls authentication processing done based on profile and personal contract information within an memory card if there is information that restricts users within each metadata
Key management	- Function that manages keys within a reception terminal
Profile management	- Function that manages profiles of individuals and terminals generated from the metadata for prior contract
Time management	- Function that manages time information in a reception terminal
Application authentication control	- Function that controls authentication with respect to plug-in applications, etc.
External equipment authentication control	- Function that controls authentication with respect to external equipment connected to a reception terminal
Communication circuit control	- Function that carries out control concerning safety of communication channels when using communication circuits and transmitting to the transmitting side information for which rights protection is needed, such as [?] history and billing information

Continued from front page

(51) Int.Cl.[7]	ID symbol		FI		Theme code (reference)
H04N	5/76		H04N	7/173	640A
	5/91		H04L	9/00	601B
	7/167		H04N	7/167	Z
	7/173	640		5/91	P

(72) Inventor Iori Yamazaki
in Broadcasting and Communication Systems
Promotion Sales Department, Hitachi Ltd.
4-6 Surugadai, Kanda, Chiyoda-ku, Tokyo

F terms (reference)

5C052	AB02	CC01	DD04	DD06	
5C053	FA20	FA28	GB05	JA21	LA11
	LA15				
5C064	BB01	BB02	BC04	BC17	BC22
	BC23	BC25	BD08	BD09	
5J104	EA10	EA17	NA02	PA05	PA11

[Publication number] Unexamined patent 2002-217894
[Gazette type] Statement of amendment under provisions of Patent Law, article 17-2
[ST gazette type] A5
[Publication date] August 2, 2002
[Application number] Pat. Appl. 2001-295722
[Issuance date] January 25, 2007
[Division and class] Division 7, class 3
[International patent classification, version 8]
H04L 9/08 F
G06F 13/00 U
G06Q 30/00 U
G06Q 50/00 U
H04N 5/76 U
H04N 7/173 U
H04N 7/167 U
H04N 5/91 U
[FI]
H04L 9/00 601 B
G06F 13/00 520 B
G06F 17/60 302 E
G06F 17/60 332
G06F 17/60 ZEC
H04N 5/76 Z
H04N 7/173 640 A
H04N 7/167 Z
H04N 5/91 P

[Procedural amendments]
[Submission date] November 30, 2006
[Procedural amendment 1]
[Document to be amended] Specification
[Item to be amended] Claims
[Method of amendment] Change
[Content of amendment]

[Claims]

[Claim 1]
In a content transmission device that transmits to the reception side content and metadata that is given to said content and is used for the playback of said content,
a data transmission device that is characterized in that it has
a metadata generation means that includes information relating to said content and generates multiple metadata in accordance with the use of said information, and
a metadata transmission means that transmits said multiple metadata to the side that receives said content, and
it generates multiple metadata to be used in playback of the content and transmits it to the reception side.
[Claim 2]
A data transmission device as described in claim 1 in which
said information relating to the content is one or more among content use contract information concerning contracts between users and businesses, content encryption key information, use restrictions information for deciding the use of the content, and information for making content viewing/storage reservations, and
said multiple metadata is one or more among metadata for prior contract including said use contract information, metadata for key distribution including said content encryption key information, metadata for storage/playback

including said use restrictions information, and metadata for EPG including content viewing/storage reservation information.

[Claim 3]

A data transmission device as described in claim 1 that further has a means that, based on content-related information of said multiple metadata, generates a metadata list for identifying said metadata information.

[Claim 4]

A data transmission device as described in claim 1 that further has a means that generates metadata for system key updating.

[Claim 5]

In a method that transmits content and metadata used in the storage and playback of said content,

a content transmission method that includes

a step that generates metadata for prior contract that includes content use contract information based on contract requests from the user side,

a step that generates metadata for key distribution including a content key that plays back content and metadata for storage/playback including content use restriction information based on content requests from the user side,

an encryption step that carries out encryption on the part of said metadata for prior contract and said metadata for storage/playback that is taken to request protection,

a step that transmits metadata that include said encryption part to the user side, and

a step that based on content reception requests from the user side encrypts content by said content key and transmits it to the user side.

[Claim 6]

Being a content reception device that receives content and multiple metadata that is given to said content and corresponds to information related to said content,

a content reception device that has

a means that receives content encrypted by a content key, metadata for contract including content use contract information, metadata for key distribution including the content key, and metadata for storage/playback of the content whose parts that require protection are encrypted,

a storage means that stores said reception content and said multiple metadata,

a data decryption means that cancels and decrypts the encryption of said multiple metadata,

a content decryption means that based on said metadata reads the content of the storage means and decrypts said read content by said content key,

a display means that displays the content decrypted by said content decryption means, and

a means that encrypts and stores in said storage means the content and metadata that are decrypted by said content decryption means and said metadata decryption means.

[Claim 7]

In a content transmission and reception system that transmits and receives content and metadata that is given to said content and is used for the playback of said content,

a content transmission and reception system that has

a metadata generation means that includes information relating to said content and generates multiple metadata that corresponds to said information,

a metadata transmission means that transmits said multiple metadata to the side that receives said content,

a reception means that receives said content and said multiple metadata,

a storage means that stores said reception content and said multiple metadata, [sic; unindented]

a data decryption means that cancels and decrypts the encryption of said multiple metadata,

a content decryption means that based on said metadata reads the content of the storage means and decrypts said read content by said content key,

a display means that displays the content decrypted by said content decryption means, and

a means that encrypts and stores in said storage means the content and metadata that are decrypted by said content decryption means and said metadata decryption means. [Procedural amendment 2] [sic; improperly formatted]

[Document to be amended] Specification
[Item to be amended] 0004
[Method of amendment] Change
[Content of amendment]

[0004]

[Problems that the invention is to solve]

To provide a content transmission service system, method, and device that can prevent data tampering and illicit use, etc. of distributed content, etc. [Procedural amendment 3] [sic; improperly formatted]

[Document to be amended] Specification
[Item to be amended] 0005
[Method of amendment] Deletion
[Content of amendment]

[Procedural amendment 4]
[Document to be amended] Specification
[Item to be amended] 0007
[Method of amendment] Change
[Content of amendment]

[0007]

[Means of solving the problems]

This invention has been given a composition in which metadata that is given to the content and is used for the playback of said content is multiply generated in accordance with the use of the content-related information and is transmitted to the content reception side. [Procedural amendment 5] [sic; improperly formatted]

[Document to be amended] Specification
[Item to be amended] 0008
[Method of amendment] Deletion
[Content of amendment]

[Procedural amendment 6]
[Document to be amended] Specification
[Item to be amended] 0009
[Method of amendment] Change
[Content of amendment]

[0009]

Also, this invention has been given a composition in which are provided a storage means that stores the elements that constitute the content and said metadata, a first decryption means that decrypts said encrypted content, a second decryption means that decrypts the encrypted data of said metadata, a means that supplies to outside media the played-back content decrypted by said first decryption means, and a means (309) that encrypts the data decrypted by said first and second decryption means or the data that is generated within the device. [Procedural amendment 7] [sic; improperly formatted]

[Document to be amended] Specification
[Item to be amended] 0083
[Method of amendment] Change
[Content of amendment]

[0083]

[Effects of the invention]

With this invention, by multiply generating and transmitting, in accordance with the use of the content-related information, metadata to be used for the playback of content, the illicit use, etc. of content on the reception side can be surely prevented.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－217894
（P2002－217894A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	13/00	５２０Ｂ　５Ｃ０５２
Ｇ０６Ｆ	13/00	５２０		17/60	３０２Ｅ　５Ｃ０５３
	17/60	３０２			３３２　５Ｃ０６４
		３３２			ＺＥＣ　５Ｊ１０４
		ＺＥＣ	Ｈ０４Ｎ	5/76	Ｚ

審査請求　未請求　請求項の数17　ＯＬ　（全 43 頁）　最終頁に続く

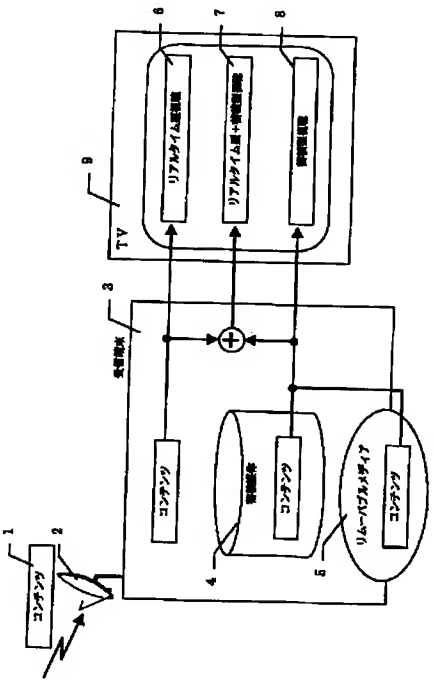
(21)出願番号　特願2001－295722(P2001－295722)
(22)出願日　平成13年９月27日(2001.9.27)
(31)優先権主張番号　特願2000－300566(P2000－300566)
(32)優先日　平成12年９月28日(2000.9.28)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　原田　宏美
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内
(72)発明者　小西　薫
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内
(74)代理人　100107010
弁理士　橋爪　健

最終頁に続く

(54)【発明の名称】　データ配信サービス方法

(57)【要約】
【課題】　コンテンツに関する詳細な情報を用いてのコンテンツ制御サービスを行う。
【解決手段】　放送サイドで視聴者へのコンテンツ提示方法、利用条件、暗号化状態でのコンテンツ蓄積、端末に対する限定受信、個人に対する限定受信等を定義し、定義した内容をコンテンツと共に受信側に配信し、これらの定義に基づき視聴者の視聴制御、蓄積制御、コピー制御、暗号/復号制御等を行うことで著作権等のコンテンツの権利保護が可能なサービスを提供する。そのために、総合データ配信システムは、コンテンツ毎にコンテンツ関連情報であるメタデータを添付する。このメタデータには、コンテンツの名称、内容、コンテンツ内の構成等の一般的な情報や、蓄積再生処理に関する制御情報、課金処理に関する制御情報、コンテンツの復号鍵等のコンテンツ暗号方式に関する情報等の著作権保護に関する情報が記述される。



1

【特許請求の範囲】

【請求項１】衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、

送信側装置は、

コンテンツの生成後にコンテンツの暗号化を行い、

暗号化されたコンテンツをブロック分けし、

配信ストリームのペイロード部分にブロック分けした暗号化コンテンツの各エレメントを格納して、配信データ形式に組み立て、コンテンツを配信し、

コンテンツの提示方法、利用条件、コンテンツの暗号鍵を含むコンテンツの関連情報を格納したメタデータを生成して配信し、

受信端末は、

コンテンツを組み立てる場合にペイロード部分を復号せずに組み立て、暗号化されたままの状態でのコンテンツ及びメタデータを蓄積し、

受信側でコンテンツの利用に関する判断をすることによりコンテンツに対する課金制御、権利保護を行うようにしたデータ配信サービス方法。

【請求項２】請求項１のデータ配信サービス方法において、

コンテンツの暗号化はコンテンツを構成する各エレメントのデータ全体に暗号化を行い、

メタデータについては予め定められた必要部分にのみ暗号化を行うことを特徴とするデータ配信サービス方法。

【請求項３】衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、

受信端末は、ユーザーが有料事業者に対し契約した端末ID、個人ID、契約したいチャンネル又は番組又はコンテンツを含む契約要求を送出側装置に通知するステップと、

送出側装置は、通知された契約要求より事前契約用メタデータを生成し、端末ID、個人IDを非暗号化とし、有料事業者ID、事業者毎に固有の事業者鍵Kw、契約コードを含む契約情報を受信端末毎に固有の端末鍵Kmcで暗号化を行い、受信端末に配信するステップと、

受信端末は、事前契約用メタデータの非暗号化部分に格納されている端末ID、個人IDにより、端末を使用するユーザー宛の情報か否かを判断し、使用ユーザー宛と判断された場合は、受信端末内に予め格納されている端末鍵Kmcにより事前契約用メタデータを復号し、事業者鍵Kwを含む契約情報を入手するステップと、

受信端末は、入手した契約情報に基づき、契約事業者の放送するコンテンツの要求を行うステップと、

送出側装置は、暗号化コンテンツの配信と同期させ、有料事業者IDを非暗号化として含み、コンテンツを視聴する際に必要となるコンテンツの暗号鍵Kkを含む必要部分が事業者鍵Kwで暗号化された鍵配信用メタデータと、コンテンツ配信装置位置を含むコンテンツに対する利用制限情報を含む必要部分をコンテンツ鍵Kkで暗号化された蓄積/再生用メタデータとを配信するステップと、

受信端末は、暗号化コンテンツと同期させて配信される鍵配信用メタデータを受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータであると判断した場合、事前契約用メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータにより配信された契約コードとによりユーザーの契約形態内で利用可能なコンテンツかを判断し、利用可能であればコンテンツ鍵Kkを受信端末に格納し、同時に受信した蓄積/再生用メタデータの暗号化部分をコンテンツ鍵Kkにより復号し、コンテンツに対する利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータに格納されている暗号化コンテンツの配信場所の情報により暗号化コンテンツを受信するステップとを含むデータ配信サービス方法。

2

【請求項４】請求項１又は３に記載のデータ配信サービス方法において、

ユーザーに対して様々なコンテンツ単位、チャンネル単位、番組単位又はパソコンにおけるファイル単位などのエレメント単位のサービスを提供するために、送出側装置は、コンテンツの物理量を示す単位を指定し、指定した物理量をメタデータに含ませて配信することにより、受信端末が指定されたコンテンツ単位でサービスを提供可能とすることを特徴としたデータ配信サービス方法。

【請求項５】請求項１又は３に記載のデータ配信サービス方法において、

メタデータは、コンテンツのタイトル又は内容、送出側で定義した視聴者へのコンテンツ提示方法、利用条件を含む情報を含み、

送出側装置は、メタデータ自体もデータの改ざん防止、秘匿性保持のため必要部分を暗号化したのち配信し、

受信端末は、暗号化されたままの状態でメタデータを蓄積し、利用時に暗号鍵により受信端末を制御して権利保護を行うことを特徴とするデータ配信サービス方法。

【請求項６】請求項１又は３のデータ配信サービス方法において、

事前契約用メタデータは、有料放送事業者の事業者鍵Kw、契約形態に間する契約コード内容を含み、端末購入時、契約更新時又は事業者鍵Kwの更新時に配信されるメタデータであって、

EPG用メタデータは、配信予定コンテンツの確認又は予約を行うためのメタデータであり、

蓄積／再生用メタデータは、コンテンツの受信、蓄積、再生に必要な情報を含むメタデータであり、

鍵配信用メタデータは、コンテンツの暗号鍵に関する情報を配信するメタデータであり、

3

メタデータリストは、配信ストリーム中の各メタデータの配信位置を取得するためのメタデータであり、
システム鍵更新用メタデータは、全受信端末共通のシステム鍵Ksyを更新するためのメタデータであり、
送信側装置は、受信端末側での使用目的、送出側での配信タイミング、記述内容によりメタデータを、事前契約用メタデータ、EPG用メタデータ、蓄積/再生用メタデータ、鍵配信用メタデータ、システム鍵更新用メタデータ、メタデータリストに区分けして、配信することを特徴とするデータ配信サービス方法。

【請求項７】請求項６に記載のデータ配信サービス方法において、
ユーザーに対して個別に配信される事前契約用メタデータは、ユーザー個々の契約情報が格納され、全ユーザーに対して共通的に配信される各コンテンツに対する鍵配信用メタデータ、蓄積/再生用メタデータは、必要となる契約情報、利用条件等が格納され、事前契約用メタデータにより配信されたユーザー個々の契約情報と他のメタデータに含まれる契約情報とを照合してユーザーのコンテンツ利用を判断することで、ユーザー個々に対しコンテンツ単位の限定受信を行うようにしたことを特徴とするシステム。

【請求項８】請求項６に記載のデータ配信サービス方法において、
事前契約用メタデータは、ユーザー毎の契約情報や事業者毎の事業者鍵Kwを含む権利保護が必要な情報が格納され、送出側装置は、この情報を各ユーザーの所有する端末毎の端末鍵Kmc又は個人鍵Kmにより暗号化することにより情報の秘匿を守り情報を配信することを特徴とするデータ配信サービス方法。

【請求項９】請求項６に記載のデータ配信サービス方法において、
EPG用メタデータは、配信予定コンテンツの確認又は予約を行うもので、利用制限情報を含む権利保護が必要な情報が格納され、
送出側装置は、この情報を全受信端末で共通な鍵Ksyにより暗号化することによりユーザーの区別無く全ユーザーに対してメタデータ内の必要な情報の秘匿性を保持したまま配信することを特徴とするデータ配信サービス方法。

【請求項１０】請求項６に記載のデータ配信サービス方法において、
コンテンツに対する暗号鍵を含む情報を格納した鍵配信用メタデータ、コンテンツのコピーコントロール情報を含む情報を格納した蓄積再生用メタデータについて、送出側装置は、鍵配信用メタデータを事業者鍵Kw、蓄積再生用メタデータをコンテンツ毎のコンテンツ鍵Kkにより暗号化し配信することで、事業者と契約を行い事前契約用メタデータにより事業者鍵を受け取ったユーザーのみコンテンツ鍵Kkを取得可能とすることでコンテンツの権利保護を実現することを特徴とするデータ配信サービス方法。

4

【請求項１１】請求項６に記載のデータ配信サービス方法において、
鍵配信用メタデータは、コンテンツの暗号鍵に関する情報を配信するものであり、
送信側装置は、コンテンツが有料放送の場合は、その情報を事業者毎に固有の事業者鍵Kwにより暗号化し、契約者以外のユーザーも視聴可能な無料コンテンツに対するメタデータの場合は、全受信端末に共通なシステム鍵Ksyにより暗号化すること。

【請求項１２】請求項６に記載のデータ配信サービス方法において、
システム鍵更新用メタデータは、システム内の全受信端末で共通なシステム鍵を含むシステム全体で共通的な情報を更新するための情報が格納されたメタデータであり、
送信側装置は、新しいシステム鍵Ksy3を含む保護が必要な部分を予め全受信端末内で共通に用意された予備用のシステム鍵Ksy2を用いて暗号化することでユーザーの区別なくメタデータ内の必要な部分の秘匿性を保持したまま配信可能とすることを特徴とするデータ配信サービス方法。

【請求項１３】請求項６に記載のデータ配信サービス方法において、
メタデータリストは、配信中の各メタデータリストの伝送路上の配信位置を格納し、受信端末は、メタデータリストを用いてメタデータの取得を行うことを特徴とするデータ配信サービス方法。

【請求項１４】請求項６に記載のデータ配信サービス方法において、
メタデータリストにEPG用メタデータ、蓄積再生用メタデータ等の更新を識別するための情報を格納することにより更新されたメタデータのみ受信を行うことを可能とすることを特徴とするに記載のデータ配信サービス方法。

【請求項１５】請求項１又は３のデータ配信サービス方法において、
暗号化されたメタデータを、暗号化を行わないメタデータに再度埋め込み配信する場合と、別ファイルとして配信する場合とのいずれかにより配信すること。

【請求項１６】請求項１又は３のデータ配信サービス方法において、
送出側装置は、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、コンテンツを利用するためのポイント数を含む情報を元に顧客情報を生成管理し、許諾するポイント数の情報を事前契約用メタデータに格納し、契約ユーザーの受信端末に配信し、
送出側装置は、コンテンツを配信する際に同期させ、配信させる蓄積/再生用メタデータにコンテンツを利用す

る際に必要となるポイント数の情報を格納して配信し、受信端末は、コンテンツを利用する際に、事前契約用メタデータにより配信されたポイント数より蓄積/再生用メタデータに格納されている必要ポイント数を減算し、コンテンツの再生を行うことで、事前契約用メタデータで配信されたポイント数の範囲でのコンテンツを視聴することを特徴とするデータ配信サービス方法。

【請求項１７】請求項１又は３データ配信サービス方法において、

送出側装置は、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、コンテンツを利用するためのポイント数を含む情報を元に顧客情報を生成管理し、オンラインペイパービュー許諾として、課金情報送信時の送信先の情報を事前契約用メタデータに格納し、契約ユーザーの受信端末に配信し、

送出側装置は、コンテンツを配信する際に同期させ、配信させる蓄積/再生用メタデータにコンテンツを利用する際の課金情報を生成する元となる情報を格納し配信する受信端末は、コンテンツを利用する際に、蓄積/再生用メタデータに格納された課金情報を生成するための元となる情報に対し利用ユーザーのIDを含む情報を加え、事前契約用メタデータにより指定された送信先に対し地上回線を利用して送信することを特徴とするデータ配信サービス方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ提供側においてコンテンツを提供し、利用側においてコンテンツを受け取り、利用するためのデータ配信サービス方法に係り、特に、コンテンツを保護する仕組みを備え且つコンテンツにコンテンツ関連情報であるメタデータを付加して配信する仕組みを備えたデータ配信サービス方法に関する。

【０００２】

【従来の技術】従来、衛星波や地上波を用いた放送または通信は、リアルタイム放送が一般的であり、一部、蓄積型の通信が存在していた。蓄積型の放送や通信は、配信された番組や情報をユーザー自身の蓄積動作によって、大容量の蓄積媒体に蓄積することが可能である。よって、ユーザーが望む時にいつでも、番組を視聴することができる。

【０００３】リアルタイム放送のコンテンツの保護方法として、コンテンツに暗号をかける方式が一般的である。暗号をかけることにより、不正な視聴や改ざんなどが困難となる。コンテンツ暗号方式として、BSデジタル放送の限定受信方式であるCAS(Conditional Access System)がある。CASはコンテンツを第１の暗号方式で暗号化し、その暗号化コンテンツを復号するための第１の復号鍵を第２の暗号方式で暗号化する。そして、暗号化コンテンツと第１の鍵をユーザーに対して配信する。その

コンテンツを受信可能なユーザーは、予め第２の暗号方式の復号鍵である第２の復号鍵を保持している。よって、第２の復号鍵を保持しているユーザーのみ第１の復号鍵を受信することができ、第１の復号鍵を受信できたユーザーのみがコンテンツを受信することが可能である。このように、CASを用いることで、限定されたユーザーのみコンテンツを入手し視聴することが可能となり、視聴可能なユーザーをコントロールすることが可能である。また、BSデジタル放送では、コンテンツに関する情報としてSI（サービス情報）が定義されている。

【０００４】

【発明が解決しようとする課題】上述のような従来技術のCASは、リアルタイム放送で用いられている限定受信方式である。この方式はコンテンツの受信と同時にコンテンツの復号処理を行う。その際、ユーザーに対する受信コントロールは可能であるが、コンテンツを復号してしまうため再生コントロールができない。また、蓄積時にコンテンツが平文状態となってしまうのでコンテンツの保護ができない。

【０００５】また、現状の衛星デジタル放送の規格においては、コンテンツに関する情報を定義するための手段として、SIのみしか存在しない。このSIはコンテンツの関連情報ではあるがEPG（電子番組ガイド）用の情報なので、詳細に記述されているわけではない。様々なコンテンツに関する詳細な情報を定義する手段は放送規格においてはないため、コンテンツ毎の制御に基づいた木目細かいサービスを行うことができない。これにより、コンテンツに関する詳細な情報を用いてのコンテンツ制御サービスは行うことができない。また、既存型の放送はコンテンツをリアルタイムで視聴することを念頭においたサービスであるため、コンテンツの蓄積制御、コピー制御を行うための情報が乏しく蓄積型放送に使用するには不充分である。

【０００６】本発明は、以上の点に鑑み、蓄積型放送かつ、コンテンツの保護が可能となる制御情報を付加するデータ配信サービス方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の総合データ配信システムは、暗号化した状態のコンテンツを受信し、その後蓄積媒体に蓄積し、コンテンツの再生時に初めて復号する暗号方式を提供する。また、コンテンツ毎にコンテンツ関連情報であるメタデータを添付する。このメタデータには、例えば、コンテンツの名称、内容、コンテンツ内の構成等の一般的な情報や、蓄積再生処理に関する制御情報、課金処理に関する制御情報、コンテンツの復号鍵等のコンテンツ暗号方式に関する情報等の著作権保護に関する情報が記述される。これらの情報に基づき視聴者の視聴制御、蓄積制御、コピー制御、暗号/復号制御等を行う。これよりコンテンツの権利保護、ユーザーの権利保護等が可能となる。

7

【０００８】本発明の第１の解決手段によると、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、送信側装置は、コンテンツの生成後にコンテンツの暗号化を行い、暗号化されたコンテンツをブロック分けし、配信ストリームのペイロード部分にブロック分けした暗号化コンテンツの各エレメントを格納して、配信データ形式に組み立て、コンテンツを配信し、コンテンツの提示方法、利用条件、コンテンツの暗号鍵を含むコンテンツの関連情報を格納したメタデータを生成して配信し、受信端末は、コンテンツを組み立てる場合にペイロード部分を復号せずに組み立て、暗号化されたままの状態でのコンテンツ及びメタデータを蓄積し、受信側でコンテンツの利用に関する判断をすることによりコンテンツに対する課金制御、権利保護を行うようにしたデータ配信サービス方法が提供される。

【０００９】本発明の第２の解決手段によると、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、受信端末は、ユーザーが有料事業者に対し契約した端末ID、個人ID、契約したいチャンネル又は番組又はコンテンツを含む契約要求を送出側装置に通知するステップと、送出側装置は、通知された契約要求より事前契約用メタデータを生成し、端末ID、個人IDを非暗号化とし、有料事業者ID、事業者毎に固有の事業者鍵Kw、契約コードを含む契約情報を受信端末毎に固有の端末鍵Kmcで暗号化を行い、受信端末に配信するステップと、受信端末は、事前契約用メタデータの非暗号化部分に格納されている端末ID、個人IDにより、端末を使用するユーザー宛の情報か否かを判断し、使用ユーザー宛と判断された場合は、受信端末内に予め格納されている端末鍵Kmcにより事前契約用メタデータを復号し、事業者鍵Kwを含む契約情報を入手するステップと、受信端末は、入手した契約情報に基づき、契約事業者の放送するコンテンツの要求を行うステップと、送出側装置は、暗号化コンテンツの配信と同期させ、有料事業者IDを非暗号化として含み、コンテンツを視聴する際に必要となるコンテンツの暗号鍵Kkを含む必要部分が事業者鍵Kwで暗号化された鍵配信用メタデータと、コンテンツ配信装置位置を含むコンテンツに対する利用制限情報を含む必要部分をコンテンツ鍵Kkで暗号化された蓄積/再生用メタデータとを配信するステップと、受信端末は、暗号化コンテンツと同期させて配信される鍵配信用メタデータを受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータであると判断した場合、事前契約用メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータ

8

により配信された契約コードとによりユーザーの契約形態内で利用可能なコンテンツかを判断し、利用可能であればコンテンツ鍵Kkを受信端末に格納し、同時に受信した蓄積/再生用メタデータの暗号化部分をコンテンツ鍵Kkにより復号し、コンテンツに対する利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータに格納されている暗号化コンテンツの配信場所の情報により暗号化コンテンツを受信するステップとを含むデータ配信サービス方法が提供される。

【００１０】

【発明の実施の形態】１．概要

（サービス概要）本総合データ配信サービスとは、見たいコンテンツを見たい時に見たい場所で見られる情報（データ）配信サービスであり、従来のリアルタイム型（放送しているものを視聴する）デジタル放送とは異なり、リアルタイム型に限らず蓄積型の情報配信をも行うサービスである。これにより視聴者が、何時でも好きなときに蓄積されたコンテンツの中から好みのコンテンツを選んで視聴することが可能なニアビデオオンデマンド（NVOD：Near Video On Demand）的なサービスが提供される。また、リムーバブルメディア、本サービスを受信する受信端末に接続される外部機器に直接コンテンツを蓄積させるもしくは、コピーすることによりユーザーの好きな場所でのコンテンツ視聴をも提供する。さらに従来のデジタル放送サービスでは端末単位での契約等の狭い範囲でのコンテンツ利用契約形態のみであったが、本サービスではユーザー個人単位での契約等も可能な広範囲のコンテンツ利用契約形態を提供する。

【００１１】図１に、総合データ配信サービスの受信側の構成図を示す。本総合データ配信サービスの概要として、蓄積型テレビ放送について図１を用い説明する。受信側では、アンテナ２、受信端末３及びテレビ９を備える。蓄積型テレビ放送とは従来のテレビ放送と同様に放送サイド（放送局）から送られてくるコンテンツ１（番組）をアンテナ２（ケーブルでの配信、パッケージでの配信の場合もある）、受信端末３で受信しテレビ９などのモニタ装置にて配信されてくるその瞬間から視聴を行う、ここではリアルタイム型視聴６と呼ぶ場合に加え、従来のビデオデッキ等と同様に一度配信されてきたコンテンツを蓄積媒体４（ハードディスク等の大容量蓄積媒体）に蓄積後視聴する蓄積型視聴８（DVD-RAM等の可搬性に富んだリムーバブルメディア５を蓄積媒体として使用することもある）、蓄積されたコンテンツと配信中のリアルタイム視聴型のコンテンツを合わせて視聴するリアルタイム型＋蓄積型視聴７などのサービスを可能とする情報配信サービスである。

【００１２】（システム概要）図２に、総合データ配信サービスの全体システム構成図を示す。本総合データ配信サービスを行うシステムとしては、衛星放送、地上波放送など電波によるインフラの他にケーブルテレビ、イ

ンターネットなどの通信線を利用したインフラでのサービスが可能であるが、本発明では一例として、図２のような衛星を利用したデジタル衛星放送をインフラとした場合について述べる。

【００１３】総合データ配信サービスが提供されるシステムの概要について図２を用い説明する。本総合データ配信サービスのシステムは送出側１００、受信側２００、送出側１００と受信側２００を結ぶ伝送路である衛星を利用した衛星回線１０、地上回線１１、流通網１２、携帯電話網１３を備える。ここでいう受信側２００とは、必ずしも家庭２０１に設置される受信端末３のみでなく、自動販売機のような公衆端末２０２、コンビニエンスストア等の店舗２０３に設置される端末、移動体である自動車等に搭載される車載端末２０４、携帯端末２０５等も想定する。送出側１００では、コンテンツ１及び制御情報等を制作、管理し受信側２００へ配信する配信センタ、コンテンツの暗号化等に使用する鍵を生成管理する鍵管理センタ、受信側のユーザーの情報を管理する顧客管理センタ、受信側のユーザーからのリクエスト、視聴履歴収集等の地上回線１１、携帯電話２０６を利用した通信を管理する地上回線管理センタ、ユーザー、販売店等に対してDVD等のパッケージメディアによるコンテンツの配信（配達）を行う物流管理センタ等を備える。

【００１４】（サービス内容）次に図２のシステムにおいて行われるサービスについて説明する。本総合データ配信サービスにおけるサービスとしては、例えば、第１に前述したように衛星デジタル回線１０を主に利用しデジタル情報としての、ビデオ、音楽、電子雑誌、ゲーム等の映像、音声、データによる総合データを家庭に設置される受信端末３に向けて配信する家庭向けサービス３００がある。第２に、家庭向けサービス３００と同様に自動販売機２０２、販売店２０３に対しデータを配信し、家庭内で容量的に蓄積しきれないデータ、蓄積をしていないデータのバックアップ、自動販売機、販売店のみで販売可能なデータ等を扱い、例えば販売店でのみ販売可能な電子雑誌を購入し、家庭の受信端末３で視聴を行う自動販売機/販売店向けサービス３０１がある。第３に、車載機器２０４、携帯端末２０５などの外部機器に対し家庭内の受信端末３、もしくは自動販売機２０２、販売店２０３などからコンテンツを携帯し家庭外で視聴を行うことを可能とし、例えば家庭の受信端末に配信された地図データをDVD等のリムーバブルメディア、ICカードを利用することにより車載機器２０４に持ち出し車の中で利用したり、音楽データをメモリカード等のリムーバブルメディア、ICカードを利用することにより持ち出し携帯端末２０５により再生等を行う移動体向けサービス３０２がある。第４に、流通網１２を利用し衛星回線１０で配信出来ないコンテンツ等をCD-ROM、DVD-ROM等のパッケージメディアにより配信を行い、例えばドラマ等のコンテンツを受信端末より予約すると、送出側よりDVD-ROM等で家庭に対しコンテンツを宅配便等で配信するパッケージデリバリサービス３０３がある。第５に、携帯電話２０６等の通信手段を有する外部機器を利用し、送出側を介し家庭内の受信端末をコントロールすることにより例えば、携帯電話２０６の画面上のEPG（電子番組ガイド）より外出先から家庭の受信端末に対して番組予約等を行う携帯電話向けサービス３０４がある。さらに、これらに限定されず、通信インフラ整備に伴い、各種多様の幅広いサービスが可能とされる。本実施の形態では、特に家庭向けサービス３００について説明するが、他のサービスにも適用可能である。

【００１５】（権利保護方式）本総合データ配信サービスとは、直接家庭などにコンテンツを配信し、家庭内等でデジタルデータでの蓄積/コピー/再生を行うことを目的としたサービスであり、これに伴いデータの改ざん、私的利用を超えるコピー、再生等の著作権等の権利に関わる課題が生じるため、コンテンツの著作権、放送事業者、視聴者など各々の権利を保護、管理する必要がある。

【００１６】図３に、総合データ配信サービスにおける権利保護方式の説明図を示す。本総合データ配信サービスにおける権利保護方式について図３を用いて説明する。総合データ配信サービスにおける権利保護方式とは、送出側でコンテンツに対し定義した視聴者へのコンテンツの提示方法、利用条件、コンテンツの暗号鍵等の情報が格納されたメタデータ１８を、暗号化したコンテンツ（暗号化コンテンツ）１７、その他PSI/SI（Program Specific Information/Service Information）等１９と共に配信し、一方、受信端末３側の権利保護機能１６（RMP機能）によりメタデータ１８を解釈し、コンテンツ１７の受信端末３への受信制御、蓄積媒体４、リムーバブルメディア５に対する蓄積制御、コピー制御、暗号/復号制御、ＴＶ９などのモニタ装置に対する提示制御、外部機器１４に対する認証制御、個人を識別するためのICカード１５に対する認証/課金制御等を行う方式である。

【００１７】次に送出側より配信されるPSI/SI１９、コンテンツ１７、メタデータ１８について説明する。PSI/SI１９とは、従来のデジタル放送と同様に、配信中ストリームより必要なデータを取得するためのデータであり、本総合データ配信サービスでは、メタデータ、暗号化コンテンツ等を取得するために利用する。従来のデジタル放送とのサービスの区別は、PSI中のNIT（Network Information Table）内に格納されるサービスリスト記述子、PMT（Program Map Table）内に格納されるストリーム識別記述子等を利用することにより行うこととする。

【００１８】コンテンツ１７は、本総合データ配信サービスにおいて、データの改ざん、不正使用を防ぐために

蓄積媒体４、リムーバブルメディア５等に、基本的に暗号化されたままの状態で蓄積される。また総合データ配信サービスにおけるコンテンツ１７とは、概念的なものであり一定の物理量を示す単位ではなく、送出側の意図する単位で指定可能であり、指定した物理量をメタデータに記すことにより受信端末はコンテンツを認識可能となる。コンテンツは、例えば、また従来のデジタル放送と同様なチャンネルを指定すれば視聴可能な動画による映像系コンテンツと、主に蓄積したのち視聴することを主眼としたデータ系のコンテンツに分けられる。

【００１９】図５０に、映像系及びデータ系コンテンツを構成するデータの説明図の一例を示す。本総合データ配信サービスでは、コンテンツを構成するデータ群の各データをエレメントと呼ぶ。よってコンテンツは１つあるいは複数エレメントより構成されるものとなる。メタデータ１８とは、本総合データ配信サービスにおいて、例えば、送出側である放送事業者の意図する単位で指定されたコンテンツに対して付与されるコンテンツの内容、構成等の検索等に利用される一般的な情報、著作権者及び関連する権利の保護を送出側で定義した視聴者へのコンテンツ提示方法、利用条件等の情報を含む。メタデータは、これらの情報により端末を制御し、権利保護を可能とする。よって、メタデータにはコンテンツと同様、保護すべき情報が含まれるため、一部を暗号化して配信を行い、蓄積時も暗号化されたままの状態で蓄積される。また、メタデータは配信タイミング、内容により、事前契約用メタデータ、EPG用メタデータ、蓄積／再生用メタデータ、鍵配信用メタデータに分類される。

【００２０】事前契約用メタデータは、有料放送事業者毎に固有の鍵である事業者鍵や、契約した事業者の放送する番組の全てが視聴可能か、一部が視聴可能か等を受信端末側で解釈するための契約コード等が格納され、ユーザー個人宛にコンテンツの配信とは非同期に配信される。EPG用メタデータは、受信端末側で配信予定のコンテンツの確認、視聴/蓄積予約を行うために必要となるコンテンツの名称、内容、放送予定日などの情報が格納され、受信端末を使用するユーザーの区別なく対象となるコンテンツの配信以前に全受信端末に向け配信され、主に受信端末のEPG表示、視聴/蓄積予約等を行うためのものである。蓄積/再生用メタデータは、コンテンツの受信、蓄積、コンテンツに対する視聴契約を行うための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向け対象となるコンテンツの配信と同期させ配信される。鍵配信用メタデータは、コンテンツの暗号化を行った鍵の情報が格納され、蓄積/再生用メタデータと同様に対象となるコンテンツの配信と同期させ配信される。メタデータリストは、PSI/SIと共に利用することにより蓄積したEPG用メタデータの更新を行うための情報、配信中ストリーム群より必要なデータを取得するための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向け常時配信される。システム鍵更新用メタデータは、端末内に予め格納されているシステム全体で共通の鍵を更新するための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向けコンテンツの配信とは非同期に配信される。

【００２１】（暗号化方式）次に本総合データ配信サービスにおけるコンテンツ、メタデータの暗号化方式について説明する。本総合データ配信サービスにおけるコンテンツ、メタデータの暗号化方式は、暗号化コンテンツ、暗号化メタデータを復号せずに蓄積するため、従来のデジタル放送における配信時に暗号化を行う方式とは異なり、コンテンツ、メタデータの生成時に暗号化を行う方式である。

【００２２】図４に、総合データ配信サービスと既存サービスの暗号化方式比較の説明図を示す。本総合データ配信サービスにおける暗号化方式と従来のデジタル放送における暗号化方式の比較を図４を用いて説明する。従来方式では、コンテンツを生成２０し、その生成されたコンテンツを暗号化する前に配信時のデータ形態であるTSP２１を形成するため、ブロック分けし、TSPのペイロード部分２２にブロック分けしたコンテンツの一部２３を格納し、その後TSPのペイロード部分を暗号化２４するため、受信端末側でコンテンツを組み立てる際に、ペイロード部分を復号する必要がある。一方、本総合データ配信サービスにおける暗号化方式の場合では、送信側で、コンテンツの生成２０後にコンテンツの暗号化２５を行い、暗号化されたコンテンツをブロック分けし、TSPのペイロード部分２２にブロック分けした暗号化コンテンツの一部のブロック２６を格納し配信するため、受信端末側でコンテンツを組み立てる場合にペイロード部分を復号せずに組み立て可能となり、送出側で暗号化されたままの状態でのコンテンツ、メタデータの蓄積が可能となる。

【００２３】（コンテンツ及びメタデータの暗号化方式）図５に、コンテンツの暗号化方式の説明図を示す。また、図６に、メタデータの暗号化方式の説明図を示す。次にコンテンツ、メタデータそれぞれの暗号化イメージについてそれぞれ図５、図６を用いて説明する。本総合データ配信サービスにおけるコンテンツの暗号化は、映像系コンテンツ２７、データ系コンテンツ２８の種別に関係なく各コンテンツを構成する各エレメント毎に暗号化を行う。例えば映像系コンテンツ２７がMPEG2-Video(PES)２９、MPEG2-AAC(PES)３０の２エレメントから構成されている場合、それぞれのエレメント毎にデータ全てに暗号化を行い、暗号化エレメント３１、３２を生成する。このとき暗号化を行うための暗号鍵３３はコンテンツ内では共通な暗号鍵Kk1を使用する。本総合データ配信サービスではコンテンツ毎に割り当てられるこの暗号鍵３３をコンテンツ鍵Kk1と呼ぶ。よって、映像系コンテンツ２７とは別のコンテンツであるデータ系コ

ンテンツ２８を構成する各エレメントは別の暗号鍵３４で暗号化される。このとき暗号鍵３４には、同様に、コンテンツ内で共通な鍵Kk2を使用する。なお、コンテンツ鍵Kkは、コンテンツ鍵全体の総称である。

【００２４】本総合データ配信サービスにおけるメタデータの暗号化は、コンテンツの暗号化とは異なり暗号化が必要なメタデータの全体に暗号化を行うのではなく、図６のように暗号化が必要な部分３５のみ抽出し暗号化を行い、暗号化したデータの容量３６等の情報を加えた暗号化データ３７を生成する。また、本総合データ配信サービスでは運用によりこの暗号化データ３７を、暗号化を行わないメタデータ３８に再度埋め込み配信する場合と、別ファイルとして配信する場合とが可能である。図５１に、本総合データ配信サービスにおいてコンテンツ、前述した各メタデータを暗号化する際に使用する暗号鍵、暗号鍵についての説明図を示す。

【００２５】（限定受信方式）図７に、総合データ配信サービスにおける限定受信方式の説明図を示す。次に、本総合データ配信サービスにおいて有料放送等のコンテンツを放送事業者と契約のあるユーザーにのみ受信/蓄積させる限定受信の方式について図７を用いて説明する。本総合データ配信サービスにおける限定受信方式とは、従来のデジタル放送で使用される方式による端末毎にチャンネル単位、番組単位に行う方式とは異なり、メタデータを利用することにより端末を利用するユーザー毎に、コンテンツ単位の限定受信を可能とする。コンテンツ単位とは前述の通り、放送事業者の意図する単位であるため最小単位はエレメント単位となり、番組を構成するワンシーン等の細かい単位での限定受信が可能となる。本総合データ配信サービスにおける方式は、事前契約用メタデータ、鍵配信用メタデータにより限定受信を行う。

【００２６】まず受信側２００のユーザーが有料事業者に対し端末ID、個人ID、契約したいチャンネル、番組、コンテンツ等の契約要求３９を送出側１００に通知する。送出側１００ではユーザーより通知された契約要求より事前契約用メタデータを生成し、契約情報等の保護の必要な部分を受信端末毎に固有の端末鍵Kmcで暗号化を行い受信側２００にユーザー毎に配信する４５。受信側２００の受信端末では、事前契約用メタデータ４０の非暗号化部分に格納されている端末ID、個人IDにより端末を使用するユーザー宛の情報かを判断し、使用ユーザー宛のIDが格納されている場合は、端末内に予め格納されている端末鍵Kmc４３により事前契約用メタデータを復号し、有料事業者ID、事業者毎に固有の事業者鍵Kw４４、契約コード等により構成される契約情報を入手する。契約情報を入手したユーザーは、次に契約事業者の放送するコンテンツ１７の要求４６を行う。送出側１００では、暗号化コンテンツ１７の配信と同期させコンテンツを視聴する際に必要となるコンテンツの暗号鍵Kk３３が格納され、必要部分を事業者鍵Kw４４で暗号化された鍵配信用メタデータ４１を全端末に配信する。また、送信側１００では、コンテンツに対する利用制限情報等が格納され、必要部分がコンテンツ鍵Kk３３で暗号化された蓄積/再生用メタデータ４２を全端末に配信する。受信端末はコンテンツと同時に配信されている鍵配信用メタデータ４１を受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータ４１であると判断した場合、事前契約用４０メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータ４０により配信された契約コードによりユーザーの契約形態内で利用可能なコンテンツかを判断する。ここで、利用可能であればコンテンツ鍵Kk３３を受信端末に格納し、同時に受信した蓄積/再生用メタデータ４２の暗号化部分をコンテンツ鍵Kk３３により復号し、コンテンツに対する年齢制限等の利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータ４２に格納されている暗号化コンテンツ１７の配信場所の情報により暗号化コンテンツ１７の受信が可能となる。本総合データ配信サービスでは上記の方式により限定受信を可能とする。

【００２７】２．課金方式

次に本総合データ配信サービスにおける課金方式について説明する。本総合データ配信サービスでは、事前契約に対する課金と、コンテンツの視聴時に対する課金の大きく２通りに分けられる。

【００２８】（事前契約に対する課金）図８に、事前契約による課金方式の説明図を示す。まず事前契約に対する課金について図８を用いて説明する。事前契約に対する課金とは、送出側１００で予めユーザー登録４７により得た顧客情報を元に課金を行うため、ユーザーのコンテンツ視聴の有無に関係せずに定額の課金が可能となる課金方式である。受信端末３を購入したユーザーは、送出側１００に対し、端末ＩＤ、個人ID、契約したい事業者、契約形態、契約期間等の情報と共に決済先の銀行口座等４８の情報を葉書や電話等により通知する。送出側１００ではこれらの情報を元に顧客情報を生成管理し、契約した事業者の鍵、契約形態を示す契約コード、契約の有効期限等を格納した事前契約用メタデータ４０を生成し契約ユーザーの受信端末３に向け配信し、ユーザーの指定した口座等４８より一定期間のコンテンツ利用契約に対する課金を行う。事前契約メタデータ４０を受信したユーザーは、格納されている有効期限の範囲で契約した事業者のコンテンツの利用が可能となる。以上が本総合データ配信サービスにおける事前契約に対する課金フローである。

【００２９】（視聴契約に対する課金）次に視聴契約に対する課金について説明する。本総合データ配信サービ

スにおける視聴契約に対する課金方式では、地上回線等の受信端末より送出側の上り回線を前提とした課金方式と、上り回線を前提としない課金方式に分けられる。

【００３０】（上り回線を前提としない課金方式）図９に、上り回線を必要としない視聴契約に対する課金方式の説明図を示す。まず地上回線等の上り回線を前提としない課金方式について図９を用いて説明する。上り回線を前提としない課金方式とは、一定ポイントの利用料を事前契約の場合と同様に事前に支払い、そのポイントの範囲でコンテンツの視聴を行う方式である。但し、一定ポイントを超える場合は追加ポイントをその都度契約可能とする。具体的な手段としては、事前契約に対する課金と同様に、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、契約形態、決済先の銀行口座４８等を送出側１００に通知し契約を行う際に一定期間に対する契約ではなく、コンテンツを利用するためのポイント数４９を通知し契約を行う。送出側１００では、これらの情報を元に顧客情報を生成管理し、契約の有効期限に関する情報の代わりに許諾するポイント数の情報を事前契約用メタデータ４０に格納し契約ユーザーの受信端末３に配信する。また送出側１００ではコンテンツ１７を配信する際に同期させ配信させる蓄積/再生用メタデータ４２にコンテンツを利用する際に必要となるポイント数の情報を格納し配信する。受信端末３ではコンテンツを利用する際に、事前契約用メタデータ４０により配信されたポイント数より蓄積/再生用メタデータ４２に格納されている必要ポイント数を減算し、コンテンツの再生を行うため、事前契約用メタデータ４０で配信されたポイント数の範囲でのコンテンツの視聴が可能となる。事前契約用メタデータ４０で配信されたポイント数がなくなった場合、ユーザーは再度送出側１００と契約し、事前契約用メタデータ４０を受信することによりポイントの補充が可能となる。送出側では、ユーザーに許諾したポイント数に応じて事前に通知された指定口座等４８よりの課金が行えるため、ユーザーのコンテンツの視聴に応じた課金が可能となる。事前契約用メタデータ４０により配信されるポイント数は、基本的にICカード内に格納するが、受信端末を利用するユーザーグループに対するポイント等の場合においては受信端末内に格納することも可能である。

【００３１】（上り回線を前提とした課金方式）次に地上回線１１等の上り回線を受信端末３に接続することを前提とした課金方式について説明する。本総合データ配信サービスにおける前項のポイントに対する課金方法の拡張として、ポイントの申し込み、ポイント追加等を受信端末３に接続された地上回線１１等によりオンラインで可能にする方式と、実際に受信端末側でコンテンツを利用した際の課金情報５０が送出側１００に地上回線１１等を通じて送られ、その情報を元に課金を行う方式が存在する。

【００３２】図１０に、上り回線を使用したオンライン課金方式の説明図を示す。ここでは後者の課金情報５０による方式について図１０を用いて説明する。オンラインで課金情報５０を送出側１００に送り課金を行うための具体的な手段としては、前述した課金方式と同様に受信端末３を購入したユーザーが端末ID、個人ID、契約したい事業者、契約形態、決済先の口座４８等を送出側１００に通知する際に、一定期間、一定ポイント数に対する契約ではなく、オンラインでのコンテンツの視聴に対する課金情報５０を送るための契約を行う。本総合データ配信サービスでは、この契約をオンラインPPV許諾契約と呼ぶ。送出側１００ではこれらの情報を元に顧客情報を生成管理し、契約の有効期限、許諾ポイント数等の情報の代わりにオンラインPPV許諾として、課金情報送信時の送信先の情報等を事前契約用メタデータ４０に格納し契約ユーザーの受信端末３に配信する。また送出側１００ではコンテンツ１７を配信する際に同期させ配信させる蓄積/再生用メタデータ４２にコンテンツを利用する際に必要となる利用時の料金などの課金情報５０を生成する元となる情報を格納し配信する。受信端末ではコンテンツを利用する際に、蓄積/再生用メタデータ４０に格納された課金情報５０を生成するための元となる情報に対し利用ユーザーのID等の情報を加え、事前契約用メタデータ４０により指定された送信先に対し地上回線を利用し送信する。これにより送出側１００では契約ユーザーの受信端末３より送信された課金情報５０内の料金を事前に登録された指定口座等４８よりユーザーのコンテンツ視聴量に応じ課金可能となる。

【００３３】３．サービスフロー

図１１に、総合データ配信サービスにおけるサービスの流れの説明図を示す。次に本総合データ配信サービスにおけるサービスの流れについて図１１を用いて説明する。本総合データ配信サービスは、例えば、受信端末３購入時に添付される葉書もしくは電話等を利用したユーザー登録時の事前契約フロー１０５、送出側１００におけるコンテンツ生成１０２、メタデータ生成１０３から配信１０４までの送出側フロー１０１、コンテンツの受信、再生等の受信側フロー３３１を含む。

【００３４】（事前契約フロー）図１２に、事前契約におけるサービスフローの説明図を示す。以下に、事前契約におけるサービスフローを図１２を用いて説明する。総合データ配信サービスにおける事前契約フロー１０５とは、送出側１００におけるサービス受信ユーザ１０６の顧客情報管理１０７を行うことを目的とする。総合データ配信サービスでは有料の蓄積型コンテンツをメインとしたサービスであるため、ユーザーはコンテンツの視聴契約を行うためのICカード１５が必要となり、そのICカード１５をユーザーが取得する手段が事前契約である。前述の限定受信方式、課金方式で説明した通り、受信側２００のユーザー１０６は、端末購入時に添付され

る葉書もしくは電話等によりユーザー１０６の氏名、住所、有料放送視聴時等の決済先である銀行口座等のユーザー個人に関する個人情報および、視聴したい有料サービス、契約形態等を端末ID等の受信端末を識別する情報と共に送出側１００に登録する。送出側１００では、ユーザー登録された個人情報、契約情報、受信端末３を識別するための端末ID等の情報を元にユーザーに対し個人IDを割り振り顧客情報を生成管理１０７する。また、送信側１００では、この顧客情報を元にICカード１５に対し割り振った個人ID等の情報を格納し、ユーザー１０６に対しそれを配布し、受信端末３、配布したICカード１５に対してICカードを有するユーザー１０６が契約を行った事業者の鍵、契約形態を示す契約コード等の情報が格納された事前契約用メタデータ４０を配信する。ユーザー１０６は契約したコンテンツの利用が可能となり、送出側１００では契約ユーザーの顧客情報の管理が可能となる。

【００３５】（送出側フロー）図１３に、送出側におけるサービスフローの説明図を示す。以下に、送出側のサービスフローについて図１３を用いて説明する。総合データ配信サービスにおける送出側のサービスフローとは、例えば、コンテンツの生成１０２、番組編成２０８、コンテンツの暗号化２０９、配信フォーマット化２１２、PSI/SI生成２１０、メタデータ生成１０３、メタデータ暗号化２１１、配信１０４を含む。

【００３６】コンテンツ生成１０２とは、映像/音声/データの各エレメントよりコンテンツ１を生成することである。番組編成２０８とは、生成したコンテンツの１つあるいは複数を組み合わせることにより放送番組を制作することである。コンテンツの暗号化２０９は、番組化した各コンテンツに含まれるエレメントをコンテンツ毎の鍵であるコンテンツ鍵Kkにより暗号化し暗号化コンテンツ１７を生成することである。配信フォーマット化２１２は、暗号化コンテンツ１７、暗号化されたメタデータをエレメントの種別により配信時のデータフォーマットであるTSP化することである。PSI/SI生成２１０とは番組編成２０８を行うことにより生成される番組の運行情報等を元にPSI/SIテーブル１９を生成することである。メタデータ生成１０３とは、コンテンツ生成１０２、番組編成２０８時のコンテンツ、番組に対するタイトル、内容、構成、利用制限情報等や、コンテンツ暗号化２０９における暗号方式、暗号鍵等の情報、配信フォーッマト化２１２した際の伝送路における配信位置等の情報よりメタデータリスト２５０、EPG用メタデータ２５１、蓄積/再生用メタデータ２５２、鍵配信用メタデータ２５３の各メタデータを生成することである。メタデータ暗号化２１１とは、メタデータ生成１０３により生成された各メタデータの保護が必要な部分に対し暗号化を行うことで、暗号化EPG用メタデータ２５４、暗号化蓄積/再生用メタデータ２５５、暗号化鍵配信用メタデータ２５６を生成することである。配信２１２とは、PSI/SI、各メタデータ、暗号化コンテンツを多重化し受信側に配信することである。

【００３７】（受信側フロー）図１４に、受信側におけるサービスフローの説明図を示す。総合データ配信サービスにおける受信側のサービスフローとは、例えば、予約３３２、コンテンツ受信/蓄積３３３、視聴契約３３４、再生３３５を含む。予約３３２とは、送出側１００より配信されるEPG用メタデータ２５４を利用し、希望するコンテンツの予約を行うことである。コンテンツ受信/蓄積３３３とは、予約した情報を元にコンテンツ配信時刻に蓄積/再生用メタデータ２５５、鍵配信用メタデータ２５６、暗号化コンテンツ１７を受信し、蓄積/再生用メタデータ２５５、暗号化コンテンツ１７を蓄積することである。視聴契約３３４とは、蓄積された蓄積/再生用メタデータの利用制限情報、ICカード１５内の個人情報、契約情報等によりコンテンツの視聴契約を行うことである。再生３３５とは、視聴契約を行った情報をもとにコンテンツの再生許可等を判断し、暗号化コンテンツ１７の復号を行った後、コンテンツの再生を行うことである。

【００３８】４．送出側システム

次にこれらのサービスフローを実現させるための送出側のシステムについて説明する。

送出側システム構成

図１５に、送出側システム全体の構成図を示す。総合データ配信サービスにおける送出側システムの全体構成を図１５を用いて説明する。送出側システムは前述の通りコンテンツやメタデータの生成、暗号化、配信を行う配信センタ２２０、総合データ配信サービスシステムで使用する鍵や、IDを生成管理する鍵管理センタ２４０、ユーザー登録情報により各ユーザーの個人情報、契約情報等の顧客情報の生成管理を行う顧客管理センタ２６０、ユーザーからの視聴履歴情報/課金情報、リクエスト等の双方向通信サービス利用時の地上回線１１による接続の管理を行う地上回線管理センタ２１４、ユーザーや、販売店に対する商品等の配送など流通網１２を利用した物流の管理を行う物流管理センタ２１３等を備える。本発明では総合データ配信サービスを実現する上で特に重要となる配信センタ２２０、鍵管理センタ２４０、顧客管理センタ２６０について詳細に説明する。

【００３９】（１）配信センタ構成

図１６に、配信センタ内の構成図を示す。配信センタ２２０内の構成を図１６を用いて説明する。配信センタ２２０はコンテンツの制作を行うオーサリングシステム２２１、オーサリングシステム２２１で制作されたコンテンツより番組を編成し、運行スケジュール等を生成管理する番組構成管理システム２２２、オーサリングシステム２２１、番組構成管理システム２２２よりのコンテンツ生成時、番組編成時に生成されるコンテンツ及び番組

のタイトル、構成等の情報を元に各メタデータを生成するメタデータ生成装置２２３、番組構成管理システム２２２で生成される運行スケジュール等を元にPSI/SIを生成するPSI/SI生成装置２２４、番組構成管理システム２２２により番組編成されたコンテンツ内の各エレメントを暗号化するコンテンツ暗号化装置２２５、メタデータ生成装置２２３により生成されたメタデータの暗号化を行うメタデータ暗号化装置２２６、PSI/SI装置２２４、コンテンツ暗号化装置２２５、メタデータ暗号化装置２２６等より入力された情報を多重化し配信可能なフォーマットに変換する送出系システム２２７を備える。以下これら各構成について説明する。

【００４０】（オーサリングシステム）図１７に、オーサリングシステム内の構成図を示す。コンテンツを生成するオーサリングシステム２２１について図１７を用いて説明する。オーサリングシステム２２１とはコンテンツ１の生成および管理を行い、完成したコンテンツ、コンテンツを生成する際に生成されるコンテンツに関するタイトル、内容、コンテンツ内の構成等の情報が格納された関連ファイル２３３を番組構成管理システム２２２に受け渡すシステムである。オーサリングシステム２２１の構成としては、映像、音声、データのエレメントを制作編集する映像オーサリングツール２２８、音声オーサリングツール２２９、データオーサリングツール２３０、各オーサリングツールより出力されるエレメントよりコンテンツ１を構成し、関連ファイル２３３を生成するコンテンツ構成装置２３１、コンテンツ構成装置により生成されたコンテンツ、関連ファイル２３３を蓄積管理するためのコンテンツ管理サーバ２３２を備える。

【００４１】映像オーサリングツール２２８、音声オーサリングツール２２９、データオーサリングツール２３０、の各オーサリングツールは、VHSビデオ、レーザーディスク（登録商標）、写真等のアナログの素材入力２３４に対しデジタル化するビデオキャプチャ、スキャナー等の機能、DAT、CD、DVD等のデジタルの素材入力２３４に対して受信側の受信端末が表示可能なフォーマットへの変換機能、各デジタル素材の編集機能、コンテンツ構成装置２３１に対して制作、編集を行った各エレメントのデジタル出力機能等を有する。コンテンツ構成装置２３１は、各オーサリングツールより出力される１つあるいは複数エレメントよりコンテンツ１を構成し、同時にコンテンツ名、コンテンツID、コンテンツの内容、ジャンル、コピー制限、対象年齢、著作権等の利用制限情報、構成するエレメントのデータ形式、容量等の情報を入力することにより関連ファイル２３３を生成しコンテンツ管理サーバ２３２に蓄積する機能を有する。コンテンツ管理サーバ２３２は、コンテンツの完成を番組構成管理システム２２２に対し通知し、番組構成管理システム２２２よりコンテンツ、関連ファイル２３３の転送要求が起こった場合、番組構成管理システム２２２に対し

要求されたコンテンツ１、関連ファイル２３３を受け渡す機能を有する。但し、コンテンツ管理サーバ２３２は番組構成管理システム２２２より転送要求が無い場合においても強制的に番組構成管理システムに対しコンテンツ１、関連ファイル２３３を受け渡す機能をも有する。

【００４２】（番組構成管理システム）図１８に、番組構成管理システム内の構成図を示す。次に番組構成管理システム２２２について図１８を用いて説明する。番組構成管理システム２２２とは、オーサリングシステム２２１で生成されたコンテンツより番組を構成し、構成した番組に対する運行スケジュール等を生成管理することにより番組を編成するシステムである。番組構成管理システム２２２は、オーサリングシステム２２１内のコンテンツ管理サーバ２３２より入力されるコンテンツ１より番組を構成する番組構成装置２３５、構成された番組に対し運行スケジュール２３８を生成し、割り当てる番組運行スケジュール生成装置２３６、番組化されたコンテンツ群、それに対応する関連ファイル群、運行スケジュールを蓄積管理する番組管理サーバ２３７を備える。なお、図１７、１８のコンテンツ生成におけるコンテンツに関連する情報を纏めたファイルをコンテンツ関連情報と総称し、それを記憶したファイルが関連ファイル２３３である。

【００４３】番組構成装置２３５とは、コンテンツ管理サーバ２３２より１つあるいは複数のコンテンツ１、関連ファイル２３３より番組を構成し、番組としてのコンテンツ群、番組に対する情報、例えば番組のタイトル、番組のID、番組の内容、ジャンル、放送する事業者のID、契約に関する情報、課金に関する情報、番組内におけるコンテンツの構成等の情報をコンテンツ管理サーバ２３２より入力された関連ファイル２３３に追加し、番組管理サーバ２３７に対し蓄積する機能を有する。番組運行スケジュール生成装置２３６は、番組管理サーバ２３７に蓄積された番組に対し、放送日時、チャンネル等の放送場所に関する情報等を割り当て、運行スケジュール２３８を生成し番組管理サーバ２３７に蓄積する機能を有する。番組管理サーバ２３７は、番組構成装置２３５、番組運行スケジュール生成装置２３６より入力されたコンテンツ群１、関連ファイル群２３３、運行スケジュール２３８等を蓄積管理し、運行スケジュール２３８の情報を元に、メタデータ生成装置２２３、PSI/SI生成装置２２４に対し運行スケジュール２３８、関連ファイル群２３３を入力し、コンテンツ暗号化装置２２５に対しメタデータ生成装置２２３、PSI/SI生成装置２２４に入力した番組情報に対応するコンテンツ群及びコンテンツのID群を入力する機能を有する。

【００４４】（PSI/SI生成装置）図１９に、PSI/SI生成装置の説明図を示す。PSI/SI生成装置２２４について図１９を用いて説明する。PSI/SI生成装置２２４とは、番組構成管理システム２２２内の番組管理サーバ２３７よ

り入力される運行スケジュール２３８、関連ファイル群２３３よりMPEG2-Systemに準拠したPSI/SIの各テーブルを生成し、運行スケジュールの情報を元に送出系システム２２７に対しTSP化した各PSI/SIテーブルを入力する機能を有する。

【００４５】（メタデータ生成装置）図２０に、メタデータ生成装置の説明図を示す。次にメタデータ生成装置２２３について図２０を用い説明する。メタデータ生成装置２２３とは、番組構成管理システム２２２内の番組管理サーバ２３７より入力される関連ファイル群、運行スケジュール、鍵管理センタ２４０に対しコンテンツのIDを受け渡すことにより得られるコンテンツ鍵Kk、送出系システム２２７より入力されるコンテンツ等の伝送路における配信位置情報等を元に、メタデータリスト２５０、EPG用メタデータ２５１、鍵配信用メタデータ２５３、蓄積/再生用メタデータ２５２を生成し、メタデータリストを送出系システム２２７に出力し、その他のメタデータをメタデータ暗号化装置２２６に出力する機能を有する。送出系システムより入力されるコンテンツ等の伝送路における配信位置情報は、送出系システム２２７側の装置により配信位置であるモジュールの指定等が可能であれば必要としない場合もある。

【００４６】（コンテンツ暗号化装置）図２１に、コンテンツ暗号化装置の説明図を示す。本システムにおけるコンテンツ暗号化装置２２５について図２１を用いて説明する。コンテンツ暗号化装置２２５とは、番組構成管理システム２２２内の番組管理サーバ２３７より入力されるコンテンツ群、ID（コンテンツID）群に基づき、番組管理サーバ２３７より入力されたID（コンテンツID）を鍵管理センタ２４０に通知し、該当するコンテンツ鍵Kkを受け取り、また、コンテンツ鍵Kkにより対応するコンテンツ内の各エレメントを前述のコンテンツ暗号化方式の通り暗号化し、生成した暗号化コンテンツを送出系システム２２７に対し出力する機能を有する。

【００４７】（メタデータ暗号化装置）図２２に、メタデータ暗号化装置の説明図を示す。次にメタデータ暗号化装置２２６について図２２を用い説明する。メタデータ暗号化装置２２６とは、メタデータ生成装置２２３より入力されるEPG用メタデータ２５１、蓄積/再生用メタデータ２５２、鍵配信用メタデータ２５３、顧客管理センタ２６０より入力される事前契約用メタデータ２５９を鍵管理センタ２４０内より入力される暗号鍵情報により暗号化し、生成された暗号化メタデータを送出系システム２２７に対し出力する機能を有する。

【００４８】各メタデータの暗号化方式について、以下に説明する。EPG用メタデータ２５１については、鍵管理センタ２４０に対しEPG用メタデータ２５１に格納されたシステムIDを受け渡すことにより得られる全受信端末に共通したシステム鍵Ksy２６４により必要部分に対し暗号化が行われる。蓄積/再生用メタデータ２５２については、鍵管理センタ２４０に対し蓄積/再生用メタデータ２５２に格納されたコンテンツIDを受け渡すことにより得られるコンテンツ毎に固有のコンテンツ鍵Kk３３により必要部分に対し暗号化が行われる。鍵配信用メタデータ２５３については、メタデータ内に格納されているIDを次のように暗号化する。すなわち、無料コンテンツに対する鍵配信用メタデータ２５７であれば、システムIDを、鍵管理センタ２４０に受け渡すことにより得られるシステム鍵Ksy２６４により、必要部分に対し暗号化する。また、有料コンテンツに対する鍵配信用メタデータ２５８であれば、事業者IDを、事業者鍵Kw４４により、それぞれ必要部分に対し暗号化する。事前契約用メタデータ２５９については、鍵管理センタ２４０に対し事前契約用メタデータ２５９内に格納された端末IDを受け渡すことにより得られる端末鍵Kmc４３により必要部分に暗号化が行われる。

【００４９】よって送出系システム２２７に対しては生成された暗号化EPG用メタデータ２５４、暗号化蓄積/再生用メタデータ２５５、暗号化鍵配信用メタデータ（無料）２６１、暗号化鍵配信用メタデータ（有料）２６２、暗号化事前契約用メタデータ２６３が出力されることとなる。

【００５０】（送出系システム）図２３に、送出系システム内の構成図を示す。以下に、総合データ配信サービスにおける送出系システム２２７について図２３を用いて説明する。送出系システム２２７とは、PSI/SI生成装置２２４、コンテンツ暗号化装置２２５、メタデータ暗号化装置２２６、メタデータ生成装置２２３より入力されるPSI/SI、暗号化コンテンツ、メタデータ等のデータを、受信端末３に対し配信可能なデータに組み立てるシステムである。送出系システム２２７は、カルーセル生成装置２３９、パケタイザ２４１、多重化装置（MUX）２４２、受託放送設備２４３を備える。カルーセル生成装置２３９とは、コンテンツ暗号化装置２２５より入力されるデータ系の暗号化コンテンツ、メタデータ暗号化装置より入力される暗号化された各メタデータ、メタデータ生成装置より入力されるメタデータリストよりMPEG2-systemにおけるデータカルーセルを生成するために各データをモジュール化したのちDII、DDB化し、パケタイザ２４１に対し出力する機能を有する。パケタイザ２４１とは、コンテンツ暗号化装置より入力されるMPEG2-Video PES、MPEG2-Audio PES等の映像系の暗号化コンテンツ、カルーセル生成装置より入力されるDII、DDB等のデータをTSP形式のデータに分割し多重化装置（MUX）２４２に対し出力する機能を有する。多重化装置（MUX）２４２とは、PSI/SI生成装置２２４、パケタイザ２４１より入力されるTSPに対し送出レート等の条件により多重化を行いTSを生成し、受託放送設備２４３に出力する機能を有する。受託放送設備２４３とは、多重化装置（MUX）２４２より入力される複数TSをさらに多重化し、受

信端末３に対して配信可能なデータ形体とし送信アンテナより配信を行う機能を有する。以上が本総合データ配信サービスにおける配信センタ２２０内の構成および各構成装置の機能及びデータ生成フローである。

【００５１】（２）鍵管理センタ構成

図２４に、鍵管理センタ内の構成図を示す。次に鍵管理センタ２４０について図２４を用いて説明する。鍵管理センタ２４０とは、配信センタ２２０、顧客管理センタ２６０より登録される各IDに対する暗号鍵を生成し、各センタからの暗号鍵の要求に対して暗号鍵を受け渡すシステムである。鍵管理センタ２４０は、鍵生成装置２４４、鍵管理サーバ２４５を備える。

【００５２】（鍵生成装置）図２５に、鍵生成装置の説明図を示す。次に鍵管理センタ２４０における鍵生成装置２４４について図２５を用いて説明する。鍵生成装置２４４とは、配信センタ２２０内のメタデータ生成装置２２３より入力される複数のコンテンツID２４６よりそれぞれのIDに対応するコンテンツの暗号鍵であるコンテンツ鍵Kk３３を生成し、生成したコンテンツ鍵Kk３３をコンテンツID２４６と共に鍵管理サーバ２４５に対し出力する機能を有する。また、システム鍵Ksy２６４、事業者鍵Kw４４、端末鍵Kmc４３、個人鍵Km２６５については鍵生成装置２４４内で各暗号鍵に対するIDであるシステムID２４７、事業者ID２４８、端末ID２４９、個人ID２７０を直接指定することにより生成し、各IDと共に鍵管理サーバ２４５に対し出力する。

【００５３】（鍵管理サーバ）図２６に、鍵管理サーバの説明図を示す。次に鍵管理サーバ２４５について図２６を用いて説明する。鍵管理サーバ２４５とは、鍵生成装置２４４により生成された鍵及びIDを管理し、配信センタ２２０内のコンテンツ暗号化装置２２５、メタデータ暗号化装置２２６、メタデータ生成装置２２３、顧客管理センタ２６０内の顧客情報管理サーバ２６７よりの暗号鍵の要求に対し対応する暗号鍵を受け渡す機能を有する。例えば配信センタ２２０内のコンテンツ暗号化装置２２５より暗号鍵の要求としてコンテンツIDを受け渡された場合は、コンテンツIDに対応する暗号鍵であるコンテンツ鍵Kkを受け渡す機能である。

【００５４】（３）顧客管理センタ構成

図２７に、顧客管理センタ内の構成図を示す。次に本総合データ配信サービスシステムにおける顧客管理センタについて図２７を用いて説明する。顧客管理センタ２６０とは、ユーザー１０６からのユーザー登録情報を元に顧客情報を生成し、鍵管理センタ２４０より受け渡される暗号鍵等の情報によりICカード、事前契約用メタデータを生成し、ICカードをユーザー１０６に配布し、事前契約用メタデータを配信センタ２２０に受け渡すシステムである。顧客管理センタ２００は、顧客情報生成システム２６６、顧客情報管理システム２７１を備える。

【００５５】（顧客情報生成システム）図２８に、顧客情報生成システム内の構成図を示す。顧客管理センタ２６０における顧客情報生成システム２６６について図２８を用いて説明する。顧客情報生成システム２６６とは、ユーザー１０６が端末購入時に添付される葉書もしくは電話にて事前契約等のユーザー登録を行った情報より顧客情報を生成し、顧客情報管理システム２７１に対し出力するシステムであり、ユーザーI/F２６８、顧客情報生成装置２６９を備える。ユーザーI/F２６８とは、ユーザーからの葉書、電話等によるユーザー登録情報を受付け、登録された情報を電子化する機能を有する。顧客情報生成装置２６９とは、ユーザーI/F２６８により電子化されたユーザー登録情報を顧客情報管理システム２７１が認識可能なデータ形式である顧客情報に編集し、顧客情報管理システム２７１に対し出力する機能を有する。

【００５６】（顧客情報管理システム）図２９に、顧客情報管理システム内の構成図を示す。顧客情報管理システム２７１とは、顧客情報生成システム２６６により入力される顧客情報を元に鍵管理センタ内の鍵管理サーバ２４５に対し個人ID２７０、個人鍵２６５等を要求し、受け取った個人ID２７０、個人鍵２６５等を利用し、事前契約用メタデータ４０、ICカード１５等を生成するシステムである。顧客情報管理システム２７１は、顧客情報管理サーバ２６７、ICカード生成装置２７２、事前契約用メタデータ生成装置２７３を備える。

【００５７】顧客情報管理サーバ２６７とは、顧客情報生成システム２６６で生成された顧客情報の管理を行い、鍵管理サーバ２４５より個人鍵Km２６５、ユーザーが契約を行う事業者鍵Kw等の情報を受け取るためのユーザー情報１５０を生成し、鍵管理サーバ２４５に出力する。ユーザー情報１５０とは、例えば、ある端末IDの振られた受信側の受信端末に対し何人のユーザーが利用するか、また端末を利用するユーザーがどの放送事業者と契約を行うかを示した情報である。このユーザー情報１５０により鍵管理サーバー２４５は、管理する個人ID２７０/個人鍵Km２６５をユーザー情報に格納されているユーザー数分確保し、同じくユーザー情報に格納されている端末ID２４９に対応する端末鍵Kmc４３、各ユーザーが契約を行う事業者IDに対応する事業者鍵Kwを顧客情報管理サーバ２６７に受け渡すことが可能となる。顧客情報管理サーバ２６７は受け取った個人ID２７０、個人鍵Km２６５、端末ID２４９、端末鍵Kmc４３、事業者ID、事業者鍵Kwを顧客情報に追加することによりユーザーの使用する端末、ユーザー自身の個人情報、契約情報等の把握が可能となり顧客管理が可能となる。ICカード生成装置２７２は、顧客情報管理サーバ２６７内の顧客情報をもとに空ICカード内の所定エリアに個人ID２７０、個人鍵Kmc２６５、端末ID２４９、各ユーザーの名前、電話番号、生年月日等の個人契約情報を格納し各ユーザー１０６に配布する。事前契約用メタデータ生成装

置２７３とは、ICカード生成装置２７２と同様に顧客情報管理サーバ２６７内の顧客情報により各ユーザーの契約する事業者のID、事業者鍵Kw、契約形態を示す契約コードおよび、各ユーザーに割り振られた個人ID２７０、各ユーザーが使用する受信端末のID２４９を格納した事前契約用メタデータを生成し配信センタ内のメタデータ暗号化装置２２６に受け渡す。以上が送出側システムの構成及び、各装置間のデータフローである。

【００５８】（送出側で生成配信される情報）次に送出側で生成し、受信端末に対して配信される各メタデータについて説明する。本総合データ配信サービスにおけるメタデータの記述方式は、前述の図６におけるXML等のテキスト形式での記述、PSI/SIのようなバイナリ形式での記述が可能である。ただし、暗号化が必要な部分については受信端末内での記述内容解釈処理の向上の点で特にバイナリ形式での記述を行うが、受信端末の処理性能が高い場合は、非暗号化部分と同様にテキスト形式での記述による運用も可能である。各メタデータの記述内容、構成について説明する。

【００５９】（事前契約用メタデータ）図３０に、事前契約用メタデータの構成および格納される情報の説明図を示す。まず、事前契約用メタデータについて図３０を用いて説明する。事前契約用メタデータ２６３とは、前述の通り有料放送事業者の事業者鍵Kwや、契約形態に間する契約コード等の内容を含み、主に限定受信を行う際の判定材料に利用されるデータであり、端末購入時、契約更新時、事業者鍵Kwの更新時等に配信されるメタデータである。端末ID、個人ID等の受信端末が端末を利用するユーザー宛に送られたデータかを識別するためのユーザー識別情報２７５と、メタデータの暗号方式、暗号化部分、暗号鍵を示すID（端末ID）等のメタデータにかけられた暗号に関する暗号化情報２７６と、ユーザーの名前、電話番号、住所、決済能力、決済先、パスワード等のユーザー自身の個人情報２７７と、ユーザーが契約を行う契約事業者のID、事業者鍵Kw、契約の有効期限、契約コード、契約ポイント等の契約情報２７８等を含む。暗号化部分については、各ユーザーの決済先等の情報が格納される個人情報２７７、事業者鍵Kw等の情報が格納される契約情報２７８が該当し、ユーザーの利用する端末固有の鍵Kmc４３により送出側で暗号化され、受信端末に配信される。暗号化に使用する暗号鍵については運用により個人鍵Kmを使用することも可能である。また、運用により事前契約用メタデータに上記の情報以外に後述するメタデータ属性情報が格納されることも可能である。

【００６０】（EPG用メタデータ）図３１に、EPG用メタデータの構成および格納される情報の説明図を示す。次にEPG用メタデータ２５４について図３１を用いて説明する。EPG用メタデータ２５４とは、主にユーザーが配信予定コンテンツの確認、配信予定コンテンツの視聴/蓄積予約を行うためのメタデータであり、EPG用メタデータの配信時が蓄積/再生用メタデータ、鍵配信用メタデータの配信時と重なるため各メタデータを識別するためのメタデータID、メタデータのタイプ、メタデータのサイズ等のメタデータ属性情報２７９と、事前契約用メタデータと同様にメタデータの暗号部分に関する暗号化情報２７６と、番組のID、放送予定日時、番組の内容、ジャンル、コンテンツの構成、番組のサイズ等の番組に関する番組情報２８０と、コンテンツのID、コンテンツの内容、エレメントの構成等のコンテンツ情報２８１と、コンテンツを利用するユーザー、コンテンツ自体に対する制限情報である年齢制限、コピー制限、蓄積制限等の利用制限情報２８２等を含む。暗号化部分についてはコピー制限等の利用制限情報２８２が該当し、全ユーザーのメタデータの利用を可能とするため、全受信端末共通のシステム鍵Ksy２６４により送出側で暗号化され配信される。コンテンツ情報２８１については、総合データ配信サービスにおけるEPGの運用レベルにより格納せずに配信することも可能とする。利用制限情報についても同様に格納せずに運用を行う場合もあり、EPG用メタデータは暗号化せずに配信されることも可能である。

【００６１】（蓄積/再生用メタデータ）図３２に、蓄積/再生用メタデータの構成および格納される情報の説明図を示す。次に蓄積/再生用メタデータ２５５について図３２を用いて説明する。蓄積/再生用メタデータ２５５とは、コンテンツの受信、蓄積、再生に必要な情報を含むメタデータであり、蓄積済みコンテンツの検索時に利用される他、ユーザーのコンテンツ利用方法を制御するために利用される。蓄積/再生用メタデータは、EPG用メタデータと同様にメタデータ自体を識別するためのメタデータ属性情報２７９と、暗号化情報２７６と、番組情報２８０と、コンテンツ情報２８１と、利用制限情報２８２と、蓄積/再生用メタデータが示すコンテンツの暗号化方式、暗号鍵ID等のコンテンツ暗号化情報、コンテンツを視聴するための契約に関する、契約形態、契約による利用可能期間等の契約情報２８４と、契約による課金料金、課金タイミング等の課金情報２８５等を含む。暗号化部分については利用制限情報２８２、コンテンツの暗号化方式、暗号鍵ID等の情報が含まれるコンテンツ暗号化情報２８３、使用制限期間等の情報が含まれる契約情報２８４、課金時の料金、タイミング等が含まれる課金情報２８５が該当し、コンテンツを暗号化した鍵と同じコンテンツ鍵Kk３３により送出側で暗号化され配信される。また、蓄積/再生用メタデータにおけるコンテンツ情報２８１については、EPG用メタデータ内に格納されるコンテンツ情報にコンテンツの配信位置等の情報が追加される。

【００６２】（鍵配信用メタデータ）図３３に、鍵配信用メタデータの構成および格納される情報の説明図を示す。次に鍵配信用メタデータ２５６について図３３を用

いて説明する。鍵配信用メタデータ２５６とは、コンテンツの暗号鍵に関する情報を配信するためのメタデータであり、コンテンツが有料放送の場合は放送する事業者に契約したユーザーのみ受信可能とする限定受信を行うための情報が含まれる。鍵配信用メタデータ２５６は、他のメタデータより区別するためのメタデータ属性情報２７９と、メタデータ自体の暗号化に関する暗号化情報２７６と、コンテンツのID、コンテンツの暗号鍵Kk等のコンテンツ鍵情報２８６等を含む。暗号化部分に関してはコンテンツ鍵Kk等のコンテンツ鍵情報が送出側で暗号化され配信される。暗号鍵については、鍵配信用メタデータ２５６が有料コンテンツに対するメタデータであり、事業者に契約したユーザーのみ受信可能な限定受信を行う場合は、事業者毎に固有の事業者鍵Kw４４が使用され、契約者以外のユーザーも視聴可能な無料コンテンツに対するメタデータの場合は、全受信端末に共通なシステム鍵Ksy２６４が使用される。また、限定受信を実現させるための事業者ID、対象契約コード等の情報はコンテンツ鍵情報に格納され暗号化されて配信される。

【００６３】（メタデータリスト）図３４に、メタデータリストの構成および格納される情報の説明図を示す。次にメタデータリスト２５０について図３４を用いて説明する。メタデータリストとは、配信ストリーム中のEPG用メタデータ、蓄積/再生用メタデータ等の配信位置を取得するためのメタデータであり、PSIを補完する情報を持ち、受信端末内に蓄積したEPG用メタデータに対し配信ストリーム中のEPG用メタデータが更新された場合における差分メタデータ蓄積のための情報を含む。メタデータリスト２５０は、受信端末側で情報の更新を識別するためのバージョン等のメタデータリスト属性情報２８７と、コンテンツIDに対応するメタデータのID、EPG用メタデータ、蓄積/再生用メタデータを区別するためのメタデータタイプ、EPG用メタデータの更新を識別するためのメタデータのバージョン、配信ストリーム上の位置情報等のリスト情報２８８等を含む。メタデータリスト自体はメタデータを配信ストリームより取得するための情報であるため特に保護を必要とせず、暗号化は行わずに配信される。メタデータリストの取得方法としてはPSIテーブルにおけるPMT内に配信ストリームを指定することにより取得を行う運用とする。

【００６４】（システム鍵更新用メタデータ）図３５に、システム鍵更新用メタデータの構成および格納される情報の説明図を示す。次にシステム鍵更新用メタデータについて図３５を用いて説明する。システム鍵更新用メタデータ２８９とは、受信端末内に格納されている全受信端末共通の鍵であるシステム鍵Ksyをシステム鍵Ksy3に更新するためのメタデータである。システム鍵更新用メタデータ２８９は、他のメタデータと区別するためのメタデータ属性情報２７９と、メタデータ自体の暗号化に関する暗号化情報２７６と、更新対象となるシステム鍵に対応するシステムID、変更後のシステムID、システム鍵、更新タイミング等の情報が含まれるシステム鍵情報２９０等を含む。

【００６５】暗号化部分は、更新後のシステム鍵、変更タイミング等の情報が含まれるシステム鍵情報２９０が該当し、暗号鍵は受信端末内に予め予備用のシステム鍵として登録されているシステム鍵Ksy2を使用する。システム鍵Ksyは、システム鍵全体の総称で、通常は１つが有効である。ただし、ハック等の被害があった時に、予備のシステム鍵Ksy2を使用する。そのために、受信機には通常２つのシステム鍵Ksy1、Ksy2が内蔵されている。システム鍵Ksyの更新処理を具体的に説明するために、システム鍵Keyの実際の受信機内の構成である２つシステム鍵Key1、Key2について述べる。Key1、Key2が受信機内部に内臓されており、これらの鍵を更新等の変更をする時に、システム鍵送信側は、他のシステム鍵Key3を衛星より伝送し、受信端末では、システム鍵Ksy1がKey3に変更となる。これより実際の受信機内には、システム鍵Key2、Ksy3の２つの鍵が存在することになる。また、システム鍵Key2が実際には有効鍵となる。以上が本総合データ配信サービスにおける送出側より配信されるメタデータである。

【００６６】５．受信側システム

つぎに、上述のサービスフローを実施させる受信側システムである受信端末について説明する。

（受信端末構成）図３６に、受信端末内の構成図を示す。次に本総合データ配信サービスにおける受信側である受信端末３について図３６を用いて説明する。受信端末３は衛星を介したコンテンツ１７、PSI/SI１９、メタデータ１８等の情報をアンテナ２により受信し、TV９等のモニタ装置に出力、また蓄積媒体４内に蓄積後出力することでユーザーの視聴を可能とする。将来的にはこの受信端末３がTV９等のモニタ装置に内蔵されることもあるがここでは一例として、別装置として説明する。総合データ配信サービス用の受信端末３の大きな特徴としては、コンテンツ１７及びメタデータ１８等の情報を蓄積するための蓄積媒体４を有している他に、暗号化し配信されたデータの復号及び受信端末内で生成される重要なデータに対し暗号化を行い、著作権保護等の権利、認証、課金等の処理、制御に関わるRMP１６機能、この受信端末を利用するユーザーの個人認証、及びユーザーの属する家族等のグループ認証を行う個人認証デバイスであるICカード１５を有していることである。このRMP１６機能とは、メタデータの内容を解釈し権利保護に関わる処理の制御を行うRMPコントローラ３０６、暗号化されたメタデータを復号するメタデータ復号機能３０７、暗号化されたコンテンツを復号するためのコンテンツ復号機能３０８、受信端末内で使用する鍵を管理する鍵管理テーブル３１１、受信端末を利用するユーザーの環境を設定するためのプロファイル３１０、受信端末内でメ

タデータ等より生成されるコンテンツの視聴を許諾する情報等の保護が必要なデータを暗号化するメタデータ暗号機能３０９等を含む。蓄積媒体４は、前述のコンテンツ１７、メタデータ１８の他に、受信端末内で生成される予約情報３１３、検索/EPGテーブル３１２等の情報が格納される受信端末に固定的な大容量蓄積媒体であるハードディスクや、必要なコンテンツ、メタデータ等の情報を格納する取り外し可能なDVD-RAM、メモリカード等のリムーバブルメディアを備える。ICカード１５は、前述した個人ID２７０、個人鍵２６５、個人契約情報２７４の他に、受信端末内で生成されるコンテンツの視聴を許諾する判断材料となる許諾情報３１４等が格納される。RMP１６については、パイレーツや暗号解読などに対するセキュリティ対策としセキュリティの守られた構成よりなるが、セキュリティ強度の退化等によりモジュールごと取り替えることが可能な構成も考えられる。

【００６７】次に受信端末の特徴的な機能であるRMP１６、蓄積媒体４、ICカード１５について説明する。

（RMP）本総合データ配信サービスにおけるRMP１６機能とは、メタデータの内容を解釈し権利保護に関わる処理の制御を行うRMPコントローラ３０６、暗号化されたメタデータを復号するメタデータ復号機能３０７、暗号化されたコンテンツを復号するためのコンテンツ復号機能３０８、受信端末内で使用する鍵を管理する鍵管理テーブル３１１、受信端末を利用するユーザーの環境を設定するためのプロファイル３１０、受信端末内でメタデータ等より生成されるコンテンツの視聴を許諾する情報等の保護が必要なデータを暗号化するメタデータ暗号機能３０９等を含む。

【００６８】図５２に、RMPコントローラ３０６の行う主な制御処理について示す。RMPコントローラ３０６の主な機能としては、図示のように、例えば、受信制御、蓄積制御、コピー制御、提示制御、視聴契約制御、課金制御、個人認証制御、鍵管理、プロファイル管理、時刻管理、アプリケーション認証制御、外部機器認証制御、外部機器認証制御、通信回線制御がある。

【００６９】（メタデータ復号）図３７に、メタデータ復号機能の説明図を示す。次にメタデータ復号について図３７を用いて説明する。メタデータ復号機能３０７とは、RMPコントローラ３０６より復号要求が起こった際に、鍵管理テーブル３１１よりRMPコントローラ３０６を介して受け渡される暗号鍵を使用し、暗号化されたメタデータ等を復号する機能である。RMPコントローラ３０６は、コンテンツの受信/蓄積時、コンテンツの視聴契約時等でメタデータを復号する必要があると判断した場合、まず蓄積媒体内の暗号化されたメタデータもしくはICカード内の暗号化された個人契約情報等を複製し、各データの非暗号化部分に格納されている前述した暗号化情報内の暗号鍵IDを読み取り、暗号鍵IDを鍵管理テーブル３１１に受け渡す。鍵管理テーブル３１１は受け渡された暗号鍵IDより対応する暗号鍵を識別し、RMPコントローラ３０６に対し暗号鍵を受け渡す。RMPコントローラ３０６は、鍵管理テーブルより受け渡された暗号鍵と、メタデータをメタデータ復号機能３０７に受け渡し、復号を要求する。メタデータ復号機能３０７は、受け渡されたメタデータの暗号部分を抽出し、抽出した暗号部分をRMPコントローラ３０６より同じく受け渡された暗号鍵により復号し、非暗号化部分のメタデータの所定部分に格納し、RMPコントローラ３０６に復号したメタデータとして受け渡す。ただし、復号したデータについては前述した通り運用により非暗号化部分とデータ形式が異なる場合があるため、その際は格納せずにその後の処理を行う運用を行うこともある。以上がメタデータ復号機能３０７の復号処理である。メタデータ復号機能３０７が復号するメタデータとは、EPG用メタデータ２５４、蓄積/再生用メタデータ２５５、鍵配信用メタデータ（無料）２６１、鍵配信用メタデータ（有料）２６２、事前契約用メタデータ２６３、システム鍵更新用メタデータ２８９の各メタデータの他に、ICカードに格納される個人契約情報２７４、許諾情報３１４が挙げられる。ICカード内の情報である個人契約情報２７４、許諾情報３１４については、暗号鍵が鍵テーブルに格納されていないため、ICカード内の個人鍵Km２６５をRMPコントローラ３０６より取得し復号を行う。

【００７０】（コンテンツ復号）図３８に、コンテンツ復号機能の説明図を示す。コンテンツ復号について図３８を用いて説明する。コンテンツ復号機能３０８とは、RMPコントローラ３０６の復号要求に対し、鍵管理テーブル３１１よりRMPコントローラ３０６を介し受け取ったコンテンツの暗号鍵であるコンテンツ鍵を使用し、コンテンツ１７内の各エレメントを復号する機能であり、主にコンテンツの再生時に行われる処理である。

【００７１】（プロファイル）図３９に、プロファイルの構成図を示す。次にプロファイルについて図３９を用いて説明する。プロファイル３１０とは、事前契約用メタデータ２６３よりRMP内で生成される個人契約情報２７４の集合であり、保護の必要なデータであるため、RMP内部のセキュリティの守られた記憶エリア（セキュアメモリ）３１７に格納され、コンテンツの視聴/蓄積予約、限定受信の判定時等に使用される。プロファイル３１０は端末ユーザー全体に対する契約情報等の格納された全体プロファイル３１５と、各ユーザー毎の契約情報が格納された個人プロファイル３１６を含む。

【００７２】（鍵管理テーブル）図４０に、鍵管理テーブルの構成図を示す。鍵管理テーブルについて図４０を用いて説明する。鍵管理テーブル３１１とは、RMPコントローラ３０６より指定されるIDに対して該当する鍵を受け渡すための情報であるID及び鍵を格納したテーブルであり、保護の必要な鍵データより構成されるため、プロファイルと同様にRMP内部のセキュリティの守られた

記憶エリア（セキュアメモリ）３１７に格納される。

【００７３】（メタデータ暗号）図４１に、メタデータ暗号機能の説明図を示す。メタデータ暗号について図４１を用いて説明する。メタデータ暗号機能３０９とは、RMP１６よりICカード１５に対し事前契約用メタデータより生成した個人契約情報２７４や、蓄積/再生用メタデータより生成したコンテンツの許諾情報３１４を格納する際に、各情報をICカード１５内の個人鍵Km２６５を用いて暗号化する機能である。

【００７４】（蓄積媒体）図４２に、蓄積媒体内に格納される情報の蓄積状態の説明図を示す。次に受信端末３における蓄積媒体４に格納されるデータの蓄積状態について図４２を用いて説明する。蓄積媒体４に格納されるデータとしては、メタデータリスト２５０、EPG用メタデータ２５４、検索/EPGテーブル３１２、予約情報３１３、蓄積/再生用メタデータ２５５、コンテンツ１７、その他受信端末のOS、アプリケーション等のソフトウェア等が存在する。蓄積媒体４自体は、この例では、セキュリティの保護された構造ではないため、蓄積媒体内に格納されるデータにおいて保護の必要なデータは、暗号化状態で蓄積される。EPG用メタデータ２５４や蓄積/再生用メタデータ２５５等を受信するためのメタデータリスト２５０と、EPG用メタデータ２５４や蓄積/再生用メタデータ２５５より生成され、受信端末のEPG表示、検索処理を行うための検索/EPGテーブル３１２と、EPG用メタデータ２５４より生成されるコンテンツ視聴/蓄積予約のための予約情報３１３とは特に保護の必要とされないデータであるため暗号化せずに蓄積媒体に格納される。ただし運用において保護が必要な場合は、端末内に予め存在する端末鍵Kmc等により暗号化を行う。コンテンツの利用制限情報等が格納されたEPG用メタデータ２５４、蓄積/再生用メタデータ２５５、コンテンツ１７については送出側で暗号化された状態で蓄積され、各データが処理に必要な際はコピーを生成し、コピーを復号し利用することにより受信端末内での再暗号化処理を省くことが可能となる。

【００７５】（ICカード）図４３に、ICカード内の構成の説明図を示す。総合データ配信サービスにおいて利用されるICカード１５内の構成について図４３を用いて説明する。ICカード１５内は、セキュリティの守られた記憶エリア（セキュアメモリ）３１７と通常の記憶エリア（通常メモリ）３１８を備える。通常の記憶エリア３１８では、保護の必要でないデータもしくは、保護が必要であるが暗号化することで保護されているデータが格納され、一方、セキュリティの守られた記憶エリア３１７に格納される情報は保護が必要なデータであるがICカード内で暗号化状態で保存できない情報が格納される。セキュリティが守られた記憶エリア３１７に格納される情報としては、ユーザー個人に割り当てられた個人ID２７０、それに対応する暗号鍵である個人鍵Km２６５等が該当し、一方、通常の記憶エリア３１８に格納されるデータは、RMP１６側で暗号化された個人契約情報２７４、許諾情報３１４等が該当する。また、セキュリティの守られた記憶エリア３１７に格納された個人ID２７０、個人鍵２６５をRMP１６に受け渡す場合は、同じくセキュリティの守られた伝送路を使用し、データの受け渡しを行う。セキュリティの守られた伝送路とは、公開鍵方式等を利用することにより実現する。

【００７６】（受信端末側で生成される情報）次に総合データ配信サービスにおいて受信端末内で生成される各情報の生成時の処理について説明する。

【００７７】（プロファイル生成）図４４に、プロファイルの生成処理の説明図を示す。まず事前契約用メタデータより生成されるプロファイルについて図４４を用いて説明する。プロファイル３１０とは、事前契約用メタデータ２６２を元にRMP内部で生成される情報である。プロファイル３１０の生成は、まず、送出側より受信した事前契約用メタデータ２６３をメタデータ復号機能により復号したのち、RMPコントローラ３０６により、事前契約用メタデータ２６３のユーザー識別情報２７５内の端末ID、個人IDにより端末全体用の契約情報か、各ユーザー用の契約情報かを判定し、メタデータ復号機能により復号された個人情報２７７、契約情報２７８より必要な情報のみを抽出し個人契約情報２７４を生成する。さらに、その個人契約情報２７４を、ユーザー識別情報２７５により識別したセキュリティエリア３１７内の全体プロファイル３１５、個人プロファイル３１６の各プロファイルに格納することにより、プロファイル３１０が生成される。

【００７８】（鍵管理テーブル）図４５に、鍵管理テーブルの生成処理の説明図を示す。次に鍵管理テーブルの生成時の処理について図４５を用いて説明する。鍵管理テーブル３１１には、ユーザーの受信端末購入時に予め格納されているID、鍵情報と、ユーザーがサービス受信時に生成されるID、鍵情報が存在する。予め格納されている情報としては、端末ID２４９、端末鍵Kmc４３、システムID２４７、システム鍵Ksy２６４が存在する。なお、システム鍵Ksyは、システム鍵Ksy1～Ksy3等のシステム鍵の総称である。この例では、システムID、鍵については、運用に使用されるID、鍵情報Ksy1と、システム鍵更新時に利用される予備用のID、鍵情報Ksy2の２種類が存在する。受信側で生成もしくは更新される部分としては、システム鍵更新時のシステムID２４７、システム鍵Ksy２６４、事業者ID２４８、事業者鍵Kw４４、コンテンツID２４６、コンテンツ鍵Kk３３が該当する。生成される各ID、鍵情報は、受信端末が受信したシステム鍵更新用メタデータ２８９、事前契約用メタデータ２６３、鍵配信用メタデータ２５６内の暗号化部分に格納されているため、RMP１６内部のメタデータ復号により復号後に、RMPコントローラにより各メタデータから抽出

され、セキュリティの守られた記憶エリア３１７に格納することにより鍵管理テーブル３１１を生成する。

【００７９】（検索/EPGテーブル）図４６に、検索/EPGテーブルの生成処理の説明図を示す。検索/EPGテーブルについて図４６を用いて説明する。検索/EPGテーブル３１２とは、受信したEPG用メタデータ２５４、蓄積/再生用メタデータ２５５よりRMP内部にコピーを作成し、メタデータ復号機能により各メタデータを復号後に、RMPコントローラにより必要項目を抽出し、蓄積媒体４内の所定位置に格納することにより生成される。検索/EPGテーブル３１２は、蓄積媒体内に複数存在するEPG用メタデータ２５４、蓄積/再生用メタデータ２５５の簡易情報の集合である。また、検索/EPGテーブル３１２は、暗号化せずに蓄積媒体に格納される情報であるため、受信端末上の検索アプリケーション、EPGアプリケーションから直接アクセス可能となり、受信端末の検索スピード、EPG表示スピードの向上が可能となる。

【００８０】（予約情報）図４７に、予約情報の生成処理の説明図を示す。次に予約情報について図４７を用いて説明する。予約情報３１３とは、ユーザーの視聴/蓄積要求に対しRMP１６内部でEPG用メタデータ２５４、プロファイル３１０より生成される情報であり、暗号化せずに蓄積媒体４に格納される情報である。ユーザーより視聴/蓄積要求が起こると、RMPコントローラ３０６は、視聴要求の対象となるコンテンツに対するEPG用メタデータ２５４のコピーをRMP内部に生成し、コピーしたEPG用メタデータをメタデータ復号機能により復号する。そして、RMPコントローラ３０６は、復号したEPG用メタデータの利用制限情報と、プロファイル内の予約要求を行ったユーザーの個人契約情報とにより、コンテンツ自体の予約が可能か、ユーザーの契約形態が要求コンテンツの予約が可能かを判定し、その後蓄積媒体４内の他の予約情報３１３により登録済みの予約がないか、スケジュール的に予約が可能か等を判定する。ここで、RMPコントローラ３０６は、予約が可能であれば個人契約情報より予約を行ったユーザーの個人ID、EPG用メタデータ２５４より、コンテンツID、コンテンツサイズ、放送予定日時等、ユーザーの要求より予約の種別を抽出し予約情報３１３を生成し、蓄積媒体４内の所定位置に格納することで予約を行う。ユーザーの嗜好性を利用した自動蓄積を行わせる場合も同様に予約情報を生成する。

【００８１】（ICカード内の個人契約情報）図４８に、個人契約情報の生成処理の説明図を示す。次にプロファイル内の個人契約情報をICカードに格納する際の暗号化処理について図４８を用いて説明する。ICカード１５内の個人契約情報とは、基本的にRMP１６内のセキュリティの守られた記憶エリア上のプロファイル内に格納されている個人契約情報２７４を暗号化させたものである。RMPコントローラ３０６は、ICカード１５が挿入されたことを認識するとICカード１５内のセキュリティエリア上の個人ID２７０をセキュリティの守られた伝送路を通じて読み取り、プロファイル内の該当個人契約情報を識別する。次に、RMPコントローラ３０６は、ICカード１５内に個人契約情報が存在すれば、それを読み取りメタデータ復号機能によりそれを復号し、互いの個人契約情報の非暗号化部分に格納されるバージョンNo.を確認し、ICカードのバージョンが新しい場合は、ICカード側の暗号化された個人契約情報をRMP内にコピーし、ICカード１５よりセキュリティの守られた伝送路を通じて取得した個人鍵Km２６５を使用しメタデータ復号により個人契約情報を復号し該当するプロファイル内の個人契約情報を更新する。RMPコントローラ３０６は、逆にプロファイル側の個人契約情報２７４のバージョンが新しい場合は、ICカード１５よりセキュリティの守られた伝送路を通じて取得した個人鍵Km２６５を使用し、メタデータ暗号機能３０９により個人契約情報の必要部分を暗号化したのちICカード１５内の所定の位置に格納することにより個人契約情報の更新を行う。

【００８２】（許諾情報）図４９に、許諾情報の生成処理の説明図を示す。次に許諾情報について図４９を用いて説明する。許諾情報３１４とは、コンテンツの視聴に対しての権利情報であり、RMP１６内でICカード１５内の個人契約情報２７４と、蓄積媒体４内の蓄積/再生用メタデータ２５５のコピーより生成される。ユーザーのコンテンツに対する視聴要求が起こると、RMPコントローラ３０６は該当するコンテンツに対する蓄積/再生用メタデータ２５５のコピーをRPM１６内部に生成し、コピーした蓄積/再生用メタデータ２５５をメタデータ復号機能により復号する。蓄積/再生用メタデータを復号化した後、RMPコントローラ３０６は、ICカード１５内より暗号化された個人契約情報２７４及び、セキュリティの守られた伝送路を通じて個人鍵Km２６５を取得し、メタデータ復号により個人契約情報２７４を復号する。個人契約情報を復号化した後、RMPコントローラ３０６は、蓄積/再生用メタデータ２５５内の利用制限情報と、個人契約情報によりユーザーが視聴可能なコンテンツかを判定し、ユーザーの選択する視聴契約形態により、蓄積/再生用メタデータ内の契約情報、課金情報等より必要な項目を抽出し許諾情報３１４を生成し、ICカード１５より取得した個人鍵Kmを使用しメタデータ暗号機能３０９により暗号化したのちICカード内の所定位置に暗号化された許諾情報を格納する。また受信端末内でユーザーの嗜好性による自動蓄積予約、画面表示の変化などの処理を行わせる場合は、許諾情報内のジャンル等の情報を集計することによりユーザーの嗜好性を判断することで、処理が可能となる。以上が総合データ配信サービスにおける受信端末内で生成される情報に対する処理である。総合データ配信サービスは、前述の送出側より配信される各メタデータ、受信側である受信端末内で配信されたメタデータを利用し各情報を生成、使用する

ことによりコンテンツの著作権、その他放送事業者、ユーザー等の権利保護を可能とする。

【００８３】

【発明の効果】本発明によると、以上のように、蓄積型放送かつ、コンテンツの保護が可能となる制御情報を付加するデータ配信サービス方法を提供することができる。

【図面の簡単な説明】

【図１】総合データ配信サービスの受信側の構成図。

【図２】総合データ配信サービスの全体システム構成図。

【図３】総合データ配信サービスにおける権利保護方式の説明図。

【図４】総合データ配信サービスと既存サービスの暗号化方式比較の説明図。

【図５】コンテンツの暗号化方式の説明図。

【図６】メタデータの暗号化方式の説明図。

【図７】総合データ配信サービスにおける限定受信方式の説明図。

【図８】事前契約による課金方式の説明図。

【図９】上り回線を必要としない視聴契約に対する課金方式の説明図。

【図１０】上り回線を使用したオンライン課金方式の説明図。

【図１１】総合データ配信サービスにおけるサービスの流れの説明図。

【図１２】事前契約におけるサービスフローの説明図。

【図１３】送出側におけるサービスフローの説明図。

【図１４】受信側におけるサービスフローの説明図。

【図１５】送出側システム全体の構成図。

【図１６】配信センタ内の構成図。

【図１７】オーサリングシステム内の構成図。

【図１８】番組構成管理システム内の構成図。

【図１９】PSI/SI生成装置の説明図。

【図２０】メタデータ生成装置の説明図。

【図２１】コンテンツ暗号化装置の説明図。

【図２２】メタデータ暗号化装置の説明図。

【図２３】送出系システム内の構成図。

【図２４】鍵管理センタ内の構成図。

【図２５】鍵生成装置の説明図。

【図２６】鍵管理サーバの説明図。

【図２７】顧客管理センタ内の構成図。

【図２８】顧客情報生成システム内の構成図。

【図２９】顧客情報管理システム内の構成図。

【図３０】事前契約用メタデータの構成および格納される情報の説明図。

【図３１】EPG用メタデータの構成および格納される情報の説明図。

【図３２】蓄積/再生用メタデータの構成および格納される情報の説明図。

【図３３】鍵配信用メタデータの構成および格納される情報の説明図。

【図３４】メタデータリストの構成および格納される情報の説明図。

【図３５】システム鍵更新用メタデータの構成および格納される情報の説明図。

【図３６】受信端末内の構成図。

【図３７】メタデータ復号機能の説明図。

【図３８】コンテンツ復号機能の説明図。

【図３９】プロファイルの構成図。

【図４０】鍵管理テーブルの構成図。

【図４１】メタデータ暗号機能の説明図。

【図４２】蓄積媒体内に格納される情報の蓄積状態の説明図。

【図４３】ICカード内の構成の説明図。

【図４４】プロファイルの生成処理の説明図。

【図４５】鍵管理テーブルの生成処理の説明図。

【図４６】検索/EPGテーブルの生成処理の説明図。

【図４７】予約情報の生成処理の説明図。

【図４８】個人契約情報の生成処理の説明図。

【図４９】許諾情報の生成処理の説明図。

【図５０】映像系及びデータ系コンテンツを構成するデータの説明図。

【図５１】本総合データ配信サービスにおいてコンテンツ、前述した各メタデータを暗号化する際に使用する暗号鍵、暗号鍵についての説明図。

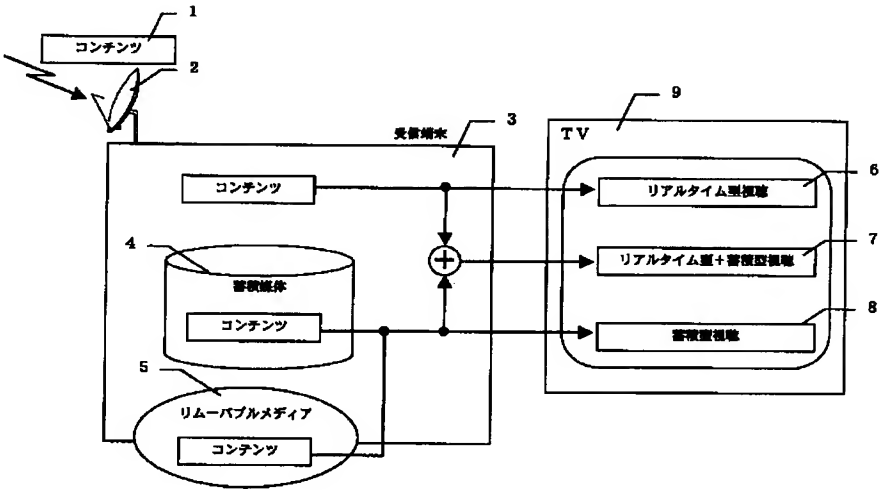
【図５２】RMPコントローラ３０６の行う主な制御処理の説明図。

【符号の説明】

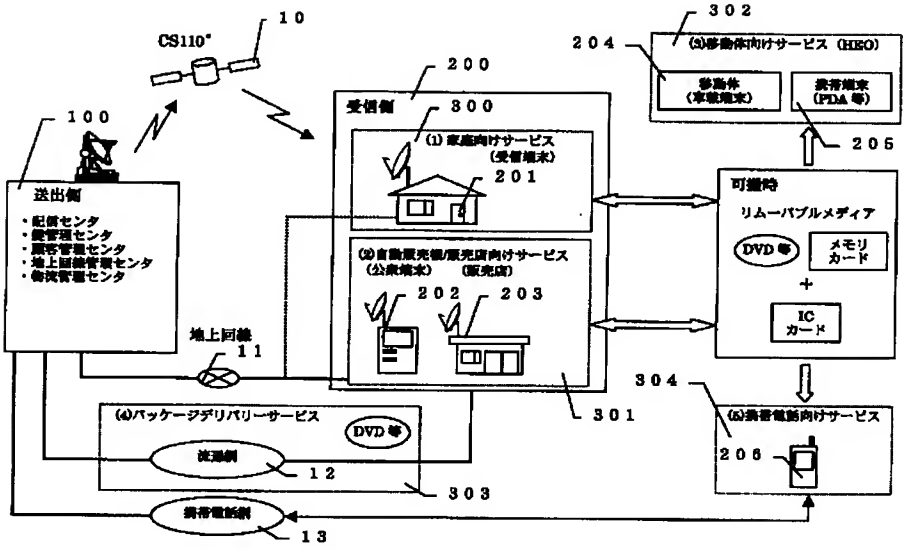
１…コンテンツ、２…アンテナ、３…受信端末、４…蓄積媒体、５…リムーバブルメディア、６…リアルタイム型視聴、７…リアルタイム型＋蓄積型視聴、８…蓄積型視聴、９…TV、１０…衛星、１１…地上回線、１２…流通網、１３…携帯電話網、１４…外部機器、１５…ICカード、１６…RMP、１７…暗号化コンテンツ、１８…暗号化メタデータ、１９…PSI/SI、２０…コンテンツ生成、２１…TSP化、２２…ペイロード、２３…コンテンツの一部、２４…ペイロード部分の暗号化、２５…コンテンツ暗号化、２６…暗号化コンテンツの一部、２７…映像系コンテンツ、２８…データ系コンテンツ、２９…MPEG2-Video (PES)、３０…MPEG2-AAC (PES)、３１…暗号化MPEG2-Video (PES)、３２…暗号化MPEG2-AAC (PES)、３３…Kk1、３４…Kk2、３５…暗号化必要部分、３６…暗号化データ容量、３７…暗号化データ、３８…非暗号化メタデータ、３９…契約要求、４０…事前契約用メタデータ、４１…鍵配信用メタデータ、４２…蓄積/再生用メタデータ、４３…端末鍵Kmc、４４…事業者鍵Kw、４５…ユーザー毎に配信、４６…コンテンツ要求、４７…ユーザー登録、４８…指定口座、４９…ポイント要求、５０…課金情報、５１…PPV登録、１００…送出

側、１０１…送出側フロー、１０２…コンテンツ生成、１０３…メタデータ生成、１０４…暗号化/配信、１０５…事前契約フロー、１０６…ユーザー、１０７…顧客管理、１５０…ユーザー情報、２００…受信側、２０１…家庭、２０２…自動販売機、２０３…販売店、２０４…車載端末、２０５…携帯端末、２０６…携帯電話、２０８…番組編成、２０９…コンテンツ暗号化、２１０…PSI/SI生成、２１１…メタデータ暗号化、２１２…配信フォーマット化、２１３…物流管理センタ、２１４…地上回線管理センタ、２２０…配信センタ、２２１…オーサリングシステム、２２２…番組構成管理システム、２２３…メタデータ生成装置、２２４…PSI/SI生成装置、２２５…コンテンツ暗号化装置、２２６…メタデータ暗号化装置、２２７…送出系システム、２２８…映像オーサリングシステム、２２９…音声オーサリングツール、２３０…データオーサリングツール、２３１…コンテンツ構成装置、２３２…コンテンツ管理サーバ、２３３…関連ファイル、２３４…素材、２３５…番組構成装置、２３６…番組運行スケジュール生成装置、２３７…番組管理サーバ、２３８…運行スケジュール、２３９…カルーセル生成装置、２４０…鍵管理センタ、２４１…パケタイザ、２４２…MUX、２４３…受託放送設備、２４４…鍵生成装置、２４５…鍵管理サーバ、２４６…コンテンツID、２４７…システムID、２４８…事業者ID、２４９…端末ID、２５０…メタデータリスト、２５１…EPG用メタデータ、２５２…蓄積/再生用メタデータ、２５３…鍵配信用メタデータ、２５４…暗号化EPG用メタデータ、２５５…暗号化蓄積/再生用メタデータ、２５６…暗号化鍵配信用メタデータ、２５７…鍵配信用メタデータ（無料）、２５８…鍵配信用メタデータ（有料）、２５９…事前契約用メタデータ、２６０…顧客管理センタ、２６１…暗号化鍵配信用メタデータ（無料）、２６２…暗号化鍵配信用メタデータ（有料）、２６３…暗号化事前契約用メタデータ、２６４…システム鍵Ksy、２６５…個人鍵Km、２６６…顧客情報生成システム、２６７…顧客情報管理サーバ、２６８…ユーザーI/F、２６９…顧客情報生成装置、２７０…個人ID、２７１…顧客情報管理システム、２７２…ICカード生成装置、２７３…事前契約用メタデータ生成装置、２７４…個人契約情報、２７５…ユーザー識別情報、２７６…暗号化情報、２７７…個人情報、２７８…契約情報、２７９…メタデータ属性情報、２８０…番組情報、２８１…コンテンツ情報、２８２…利用制限情報、２８３…コンテンツ暗号化情報、２８４…契約情報、２８５…課金情報、２８６…コンテンツ鍵情報、２８７…メタデータリスト属性情報、２８８…リスト情報、２８９…システム鍵更新用メタデータ、２９０…システム鍵情報、３００…家庭向けサービス、３０１…自動販売機/販売店向けサービス、３０２…移動体向けサービス、３０３…パッケージデリバリサービス、３０４…携帯電話向けサービス、３０６…RMPコントローラ、３０７…メタデータ復号、３０８…コンテンツ復号、３０９…メタデータ暗号、３１０…プロファイル、３１１…鍵管理テーブル、３１２…検索/EPGテーブル、３１３…予約情報、３１４…許諾情報、３１５…全体プロファイル、３１６…個人プロファイル、３１７…セキュアメモリ、３１８…通常メモリ、３３１…受信側フロー、３３２…予約、３３３…コンテンツ受信/蓄積、３３４…視聴契約、３３５…再生

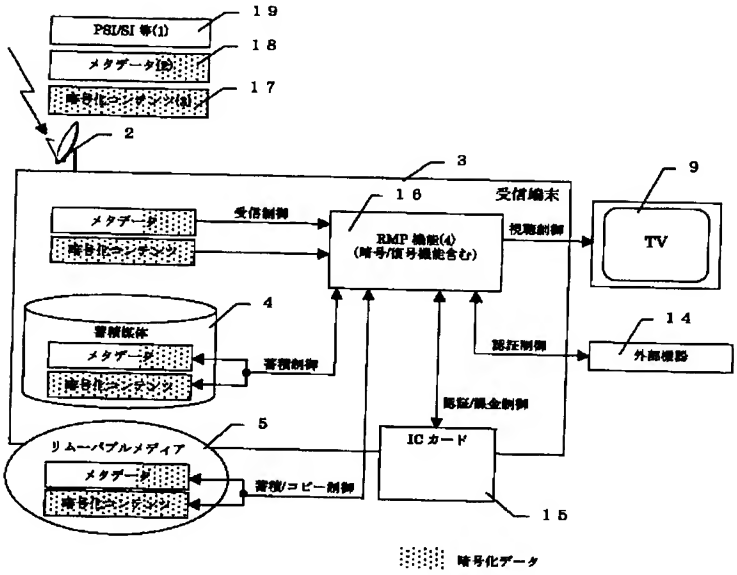
【図１】



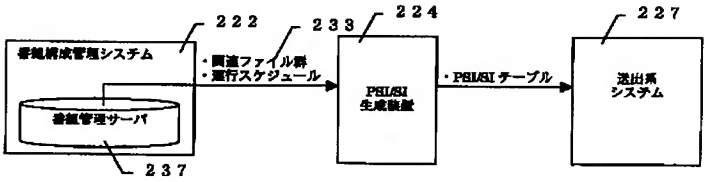
【図２】


CS110°
10
100
送出側
・配信センタ
・鍵管理センタ
・顧客管理センタ
・地上回線管理センタ
・衛星管理センタ
地上回線
11
200
受信側
300
(1)家庭向けサービス
(受信端末)
201
(2)自動販売機/販売店向けサービス
(公衆端末)
(販売店)
202
203
(4)パッケージデリバリーサービス
DVD等
流通網
12
303
携帯電話網
13
301
302
204
(3)移動体向けサービス(HSO)
移動体
(車載端末)
携帯端末
(PDA等)
205
可搬時
リムーバブルメディア
DVD等
メモリ
カード
+
IC
カード
304
(5)携帯電話向けサービス
206

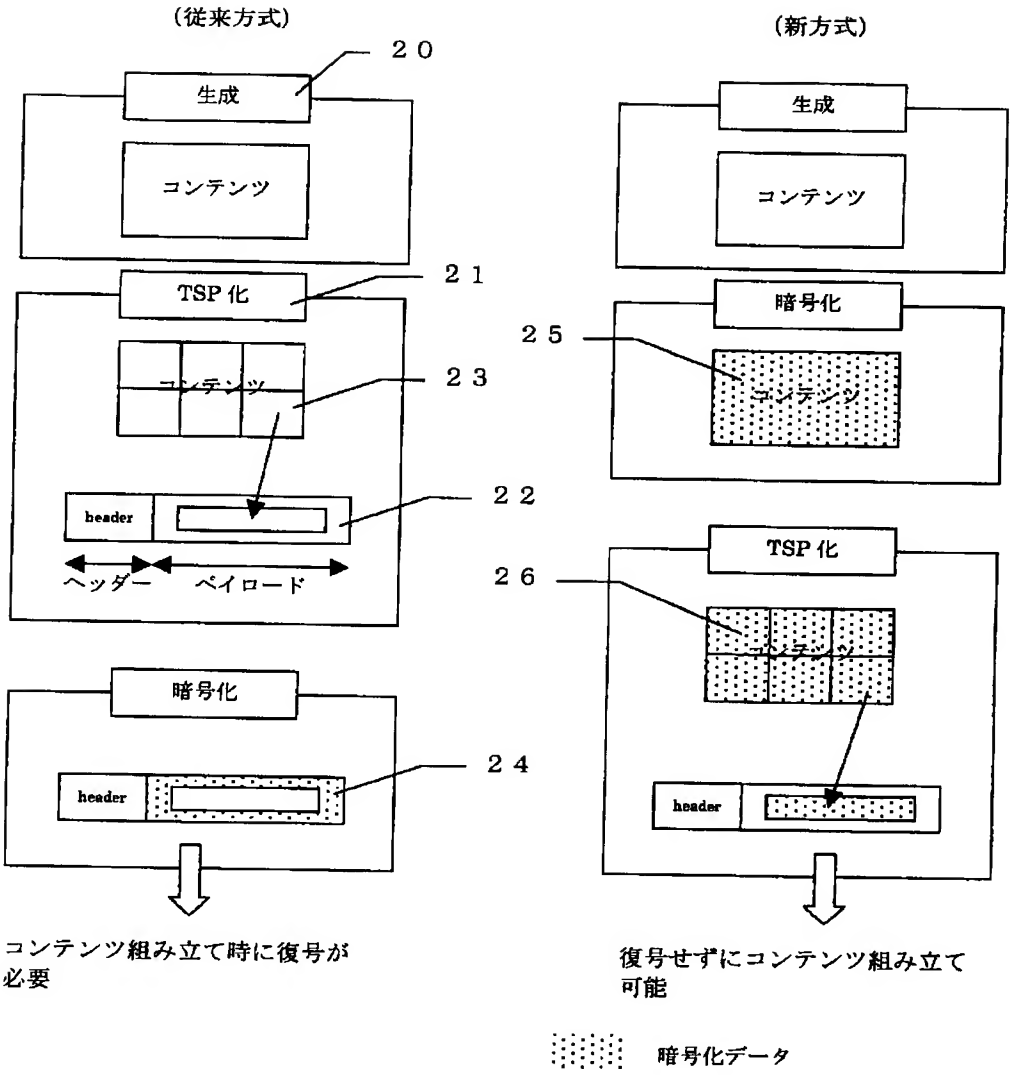
【図３】


PSI/SI等(1)
19
メタデータ(2)
18
暗号化コンテンツ(3)
17
2
3
受信端末
16
メタデータ
暗号化コンテンツ
受信制御
RMP機能(4)
(暗号/復号機能含む)
視聴制御
9
TV
4
蓄積媒体
メタデータ
暗号化コンテンツ
蓄積制御
14
課金制御
外部機器
認証/課金制御
5
リムーバブルメディア
メタデータ
暗号化コンテンツ
蓄積/コピー制御
IC カード
15
暗号化データ

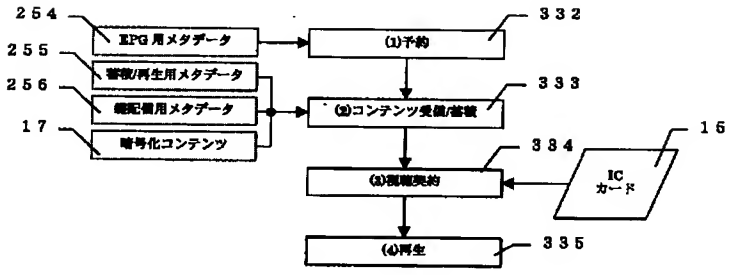
【図１９】


222
番組構成管理システム
番組管理サーバ
237
233
・周波ファイル群
・運行スケジュール
224
PSI/SI
生成装置
・PSI/SIテーブル
227
送出系
システム

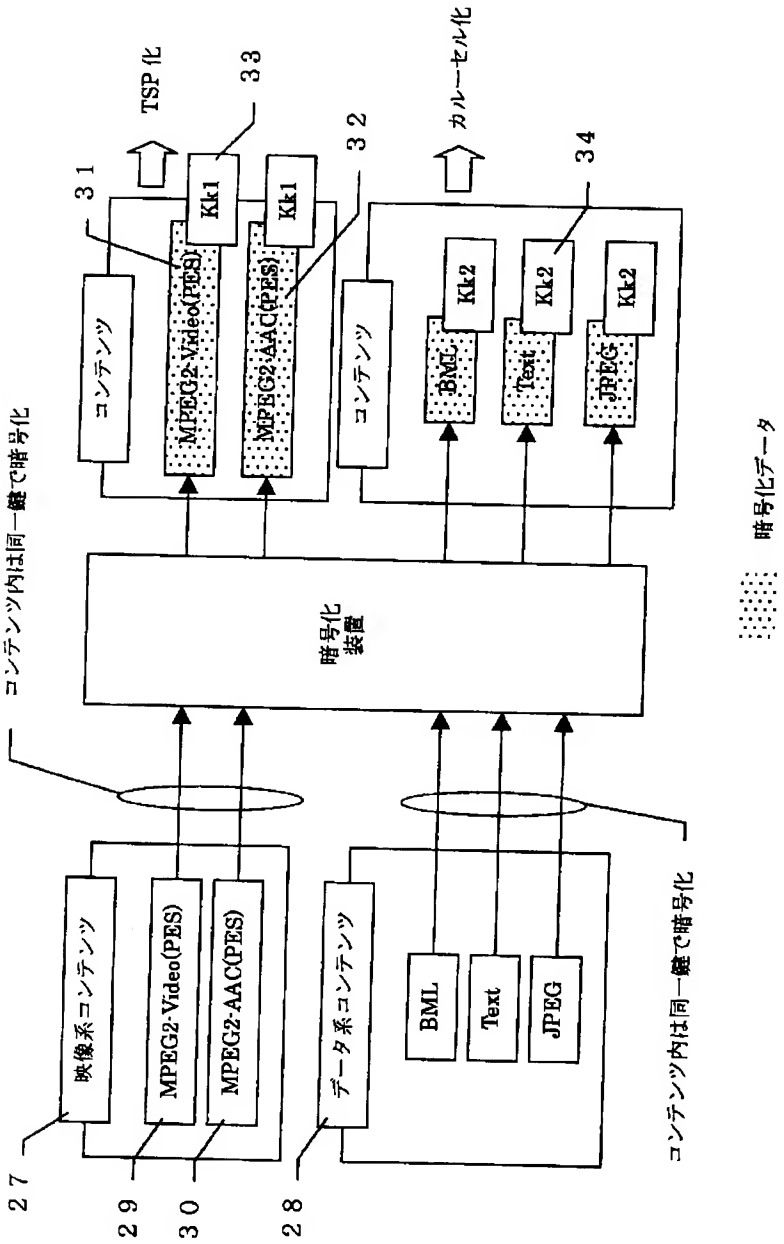
【図４】


(従来方式)
(新方式)
２０
生成
コンテンツ
２１
TSP 化
２３
コンテンツ
header
２２
ヘッダー
ペイロード
暗号化
２４
２５
２６
コンテンツ組み立て時に復号が必要
復号せずにコンテンツ組み立て可能
暗号化データ

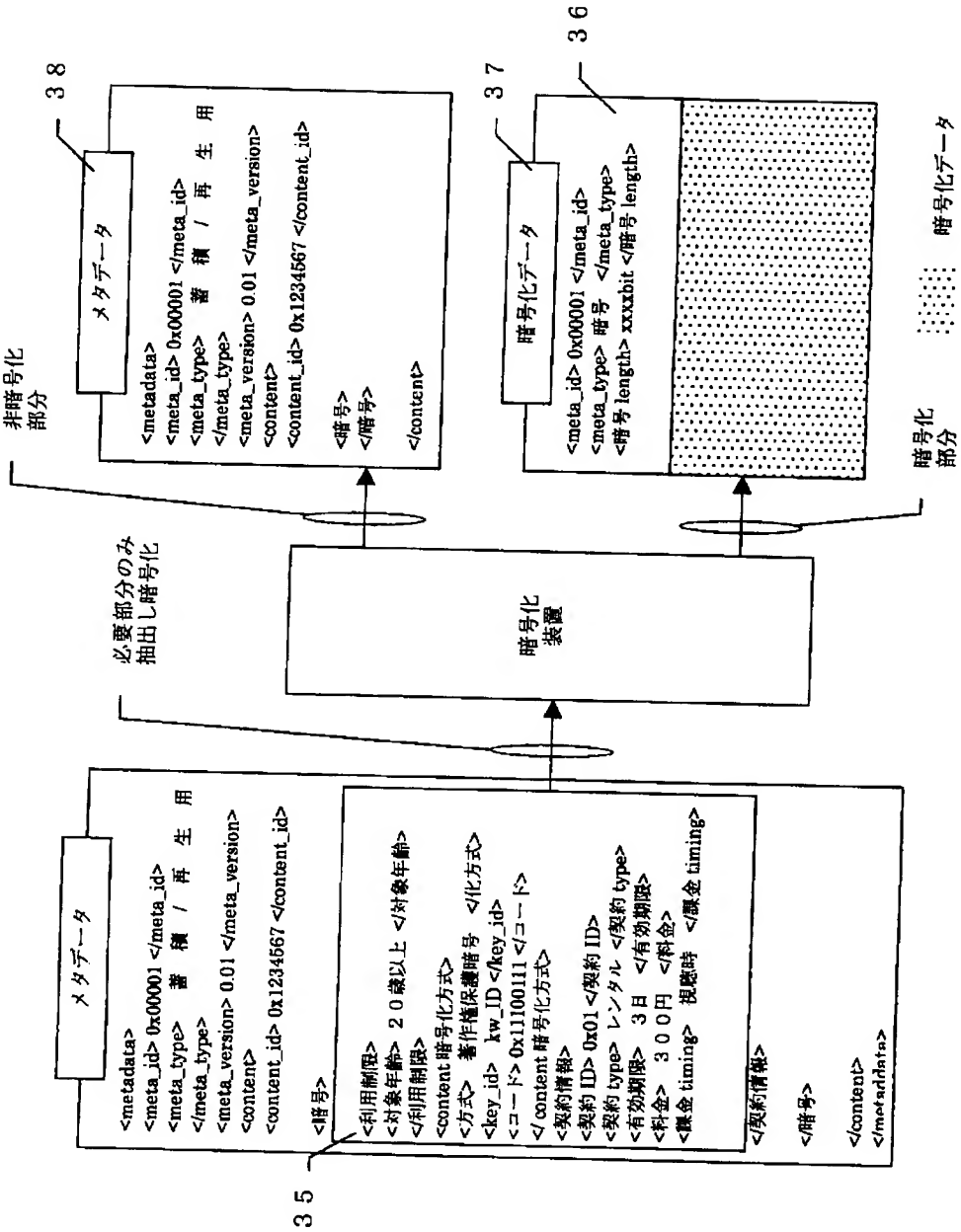
【図１４】


254
EPG 用メタデータ
255
蓄積/再生用メタデータ
256
配信用メタデータ
17
暗号化コンテンツ
(1)予約
332
(2)コンテンツ受信/蓄積
333
(3)視聴契約
334
(4)再生
335
IC カード
16

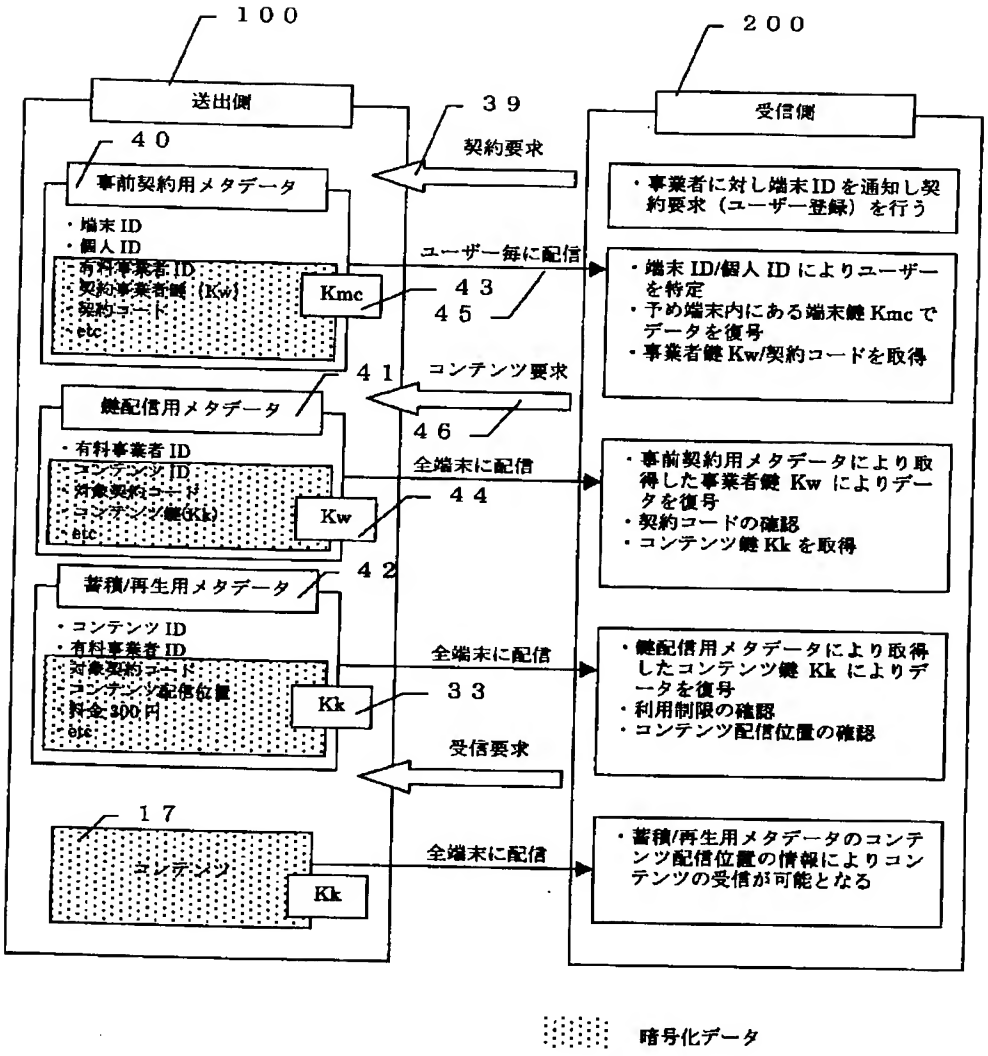
【図５】


TSP化
カルーセル化
コンテンツ内は同一鍵で暗号化
暗号化装置
映像系コンテンツ
MPEG2-Video(PES)
MPEG2-AAC(PES)
データ系コンテンツ
BML
Text
JPEG
Kk1
Kk2
コンテンツ内は同一鍵で暗号化
暗号化データ
27
28
29
30
31
32
33
34

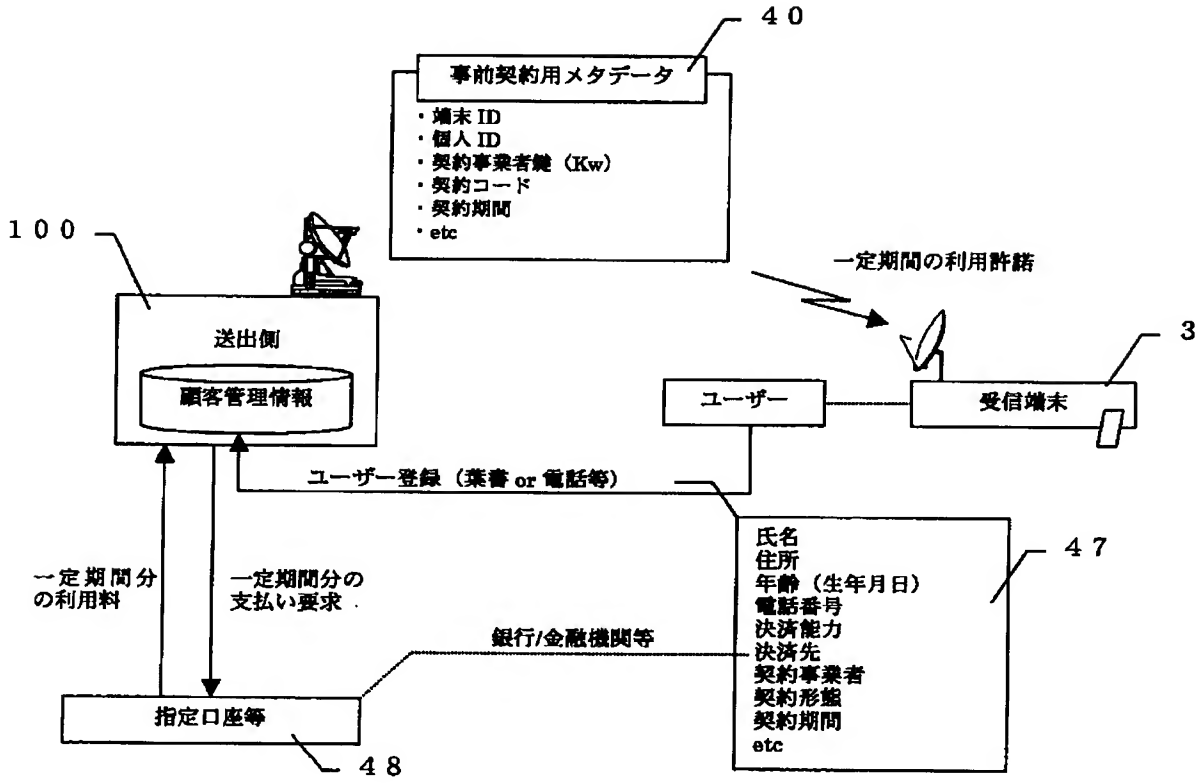
【図６】


非暗号化
部分
必要部分のみ
抽出し暗号化
暗号化
装置
暗号化
部分
暗号化データ
メタデータ
<metadata>
<meta_id> 0x00001 </meta_id>
<meta_type> 蓄積/再生用
</meta_type>
<meta_version> 0.01 </meta_version>
<content>
<content_id> 0x1234567 </content_id>
<暗号>
<利用制限>
<対象年齢> ２０歳以上 </対象年齢>
</利用制限>
<content 暗号化方式>
<方式> 著作権保護暗号 </化方式>
<key_id> kw_ID </key_id>
<コード> 0x11100111 </コード>
</content 暗号化方式>
<契約情報>
<契約 ID> 0x01 </契約 ID>
<契約 type> レンタル </契約 type>
<有効期限> ３日 </有効期限>
<料金> ３００円 </料金>
<課金 timing> 視聴時 </課金 timing>
</契約情報>
</暗号>
</content>
</metadata>
35
38
37
36
暗号化データ
<meta_id> 0x00001 </meta_id>
<meta_type> 暗号 </meta_type>
<暗号 length> xxxxbit </暗号 length>

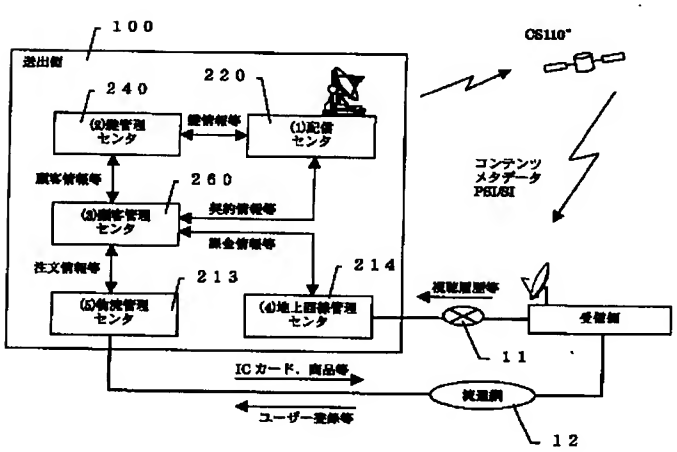
【図７】


１００
送出側
３９
契約要求
４０
事前契約用メタデータ
・端末ID
・個人ID
・有料事業者ID
・契約事業者鍵（Kw）
・契約コード
・etc
Kmc
ユーザー毎に配信
４３
４５
４１
コンテンツ要求
鍵配信用メタデータ
４６
・有料事業者ID
・コンテンツID
・対象契約コード
・コンテンツ鍵(Kk)
・etc
Kw
全端末に配信
４４
４２
蓄積/再生用メタデータ
・コンテンツID
・有料事業者ID
・対象契約コード
・コンテンツ配信位置
・料金300円
・etc
Kk
全端末に配信
３３
受信要求
１７
コンテンツ
Kk
全端末に配信
２００
受信側
・事業者に対し端末IDを通知し契約要求（ユーザー登録）を行う
・端末ID/個人IDによりユーザーを特定
・予め端末内にある端末鍵Kmcでデータを復号
・事業者鍵Kw/契約コードを取得
・事前契約用メタデータにより取得した事業者鍵Kwによりデータを復号
・契約コードの確認
・コンテンツ鍵Kkを取得
・鍵配信用メタデータにより取得したコンテンツ鍵Kkによりデータを復号
・利用制限の確認
・コンテンツ配信位置の確認
・蓄積/再生用メタデータのコンテンツ配信位置の情報によりコンテンツの受信が可能となる
暗号化データ

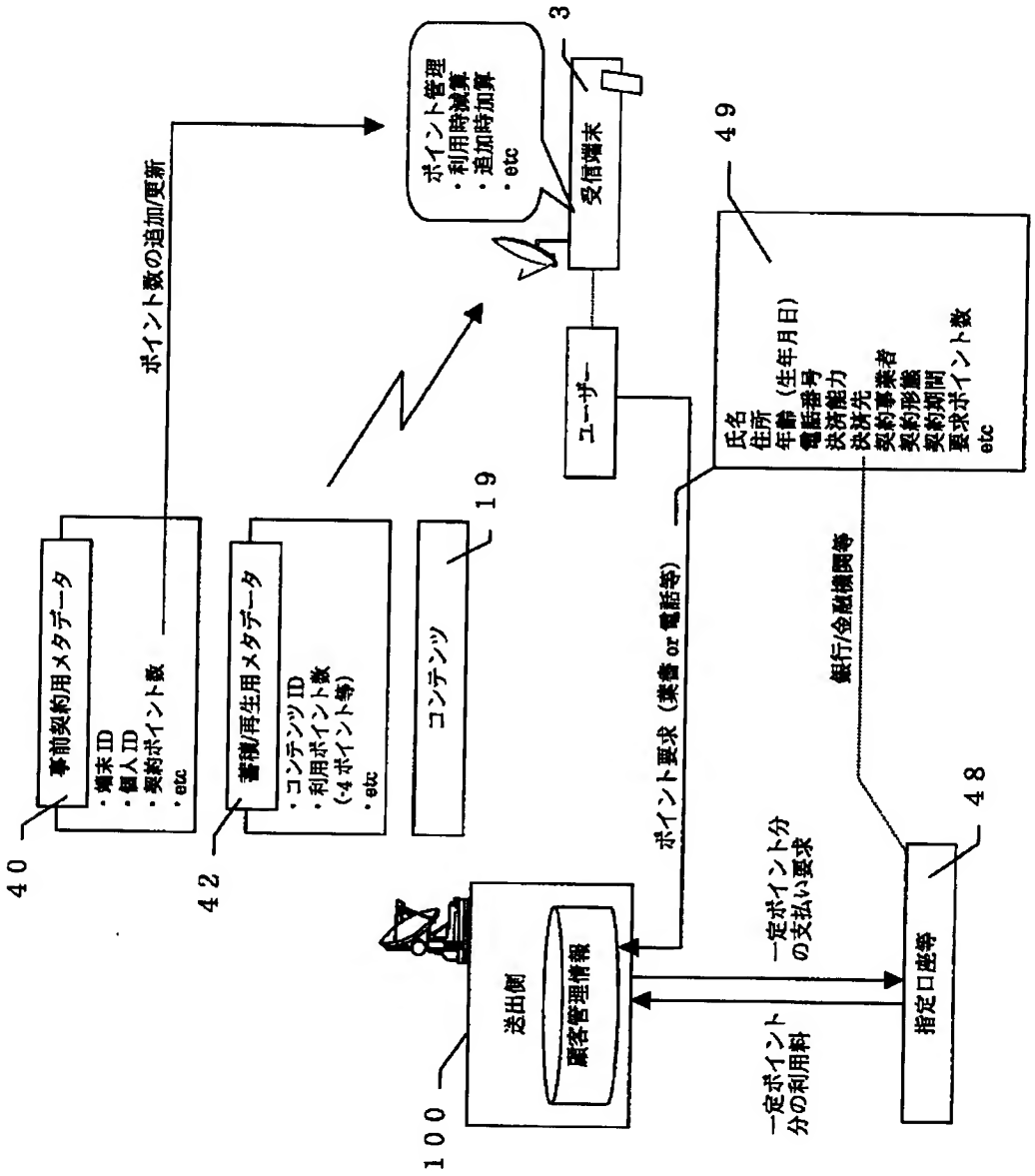
【図８】


４０
事前契約用メタデータ
・端末 ID
・個人 ID
・契約事業者鍵（Kw）
・契約コード
・契約期間
・etc
１００
送出側
顧客管理情報
一定期間の利用許諾
３
ユーザー
受信端末
ユーザー登録（葉書 or 電話等）
氏名
住所
年齢（生年月日）
電話番号
決済能力
決済先
契約事業者
契約形態
契約期間
etc
４７
一定期間分
の利用料
一定期間分の
支払い要求
銀行/金融機関等
指定口座等
４８

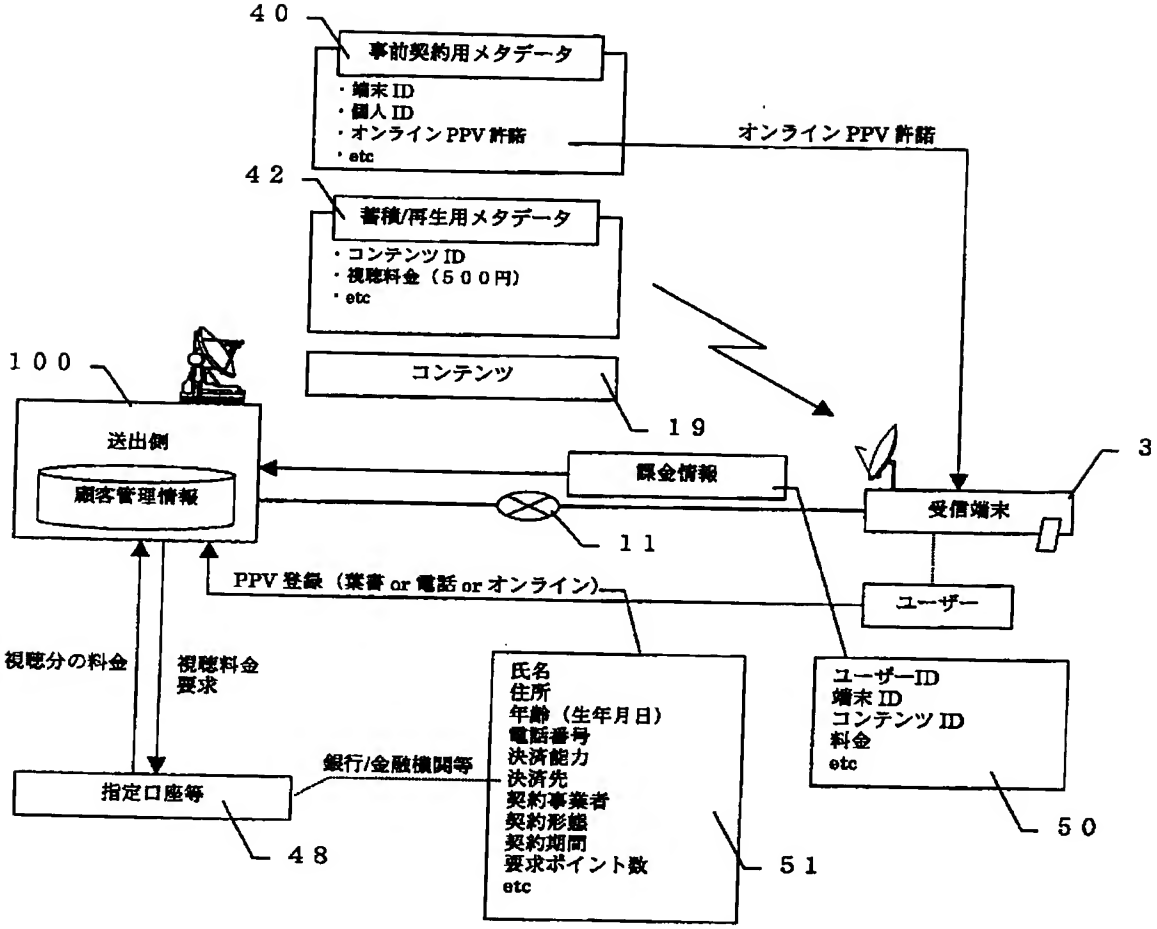
【図１５】


１００
送出側
２２０
２４０
２６０
２１３
２１４
CS110"
コンテンツ
メタデータ
PSI/SI
ICカード，商品等
ユーザー登録等
１１
１２

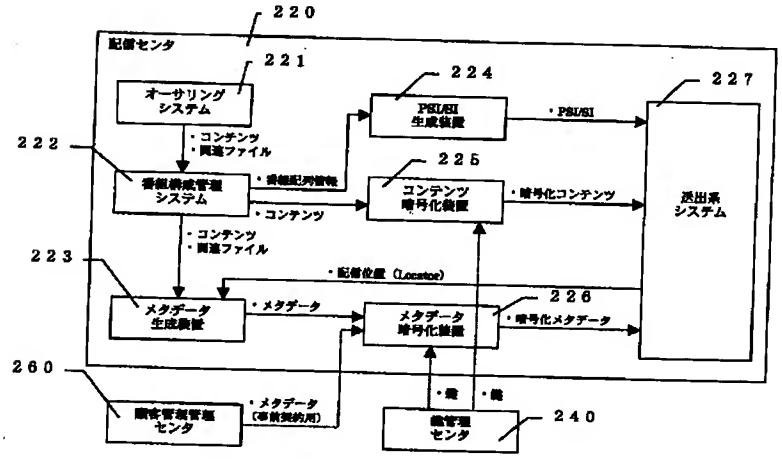
【図９】


ポイント管理
・利用時減算
・追加時加算
・etc
3
受信端末
ユーザー
49
氏名
住所
年齢（生年月日）
電話番号
決済能力
決済先
契約事業者
契約形態
契約期間
要求ポイント数
etc
ポイント数の追加/更新
事前契約用メタデータ
・端末ID
・個人ID
・契約ポイント数
・etc
40
蓄積/再生用メタデータ
・コンテンツID
・利用ポイント数
（4ポイント等）
・etc
42
コンテンツ
19
ポイント要求（課金 or 電話等）
銀行/金融機関等
48
一定ポイント分
の支払い要求
一定ポイント
分の利用料
指定口座等
送出側
顧客管理情報
100

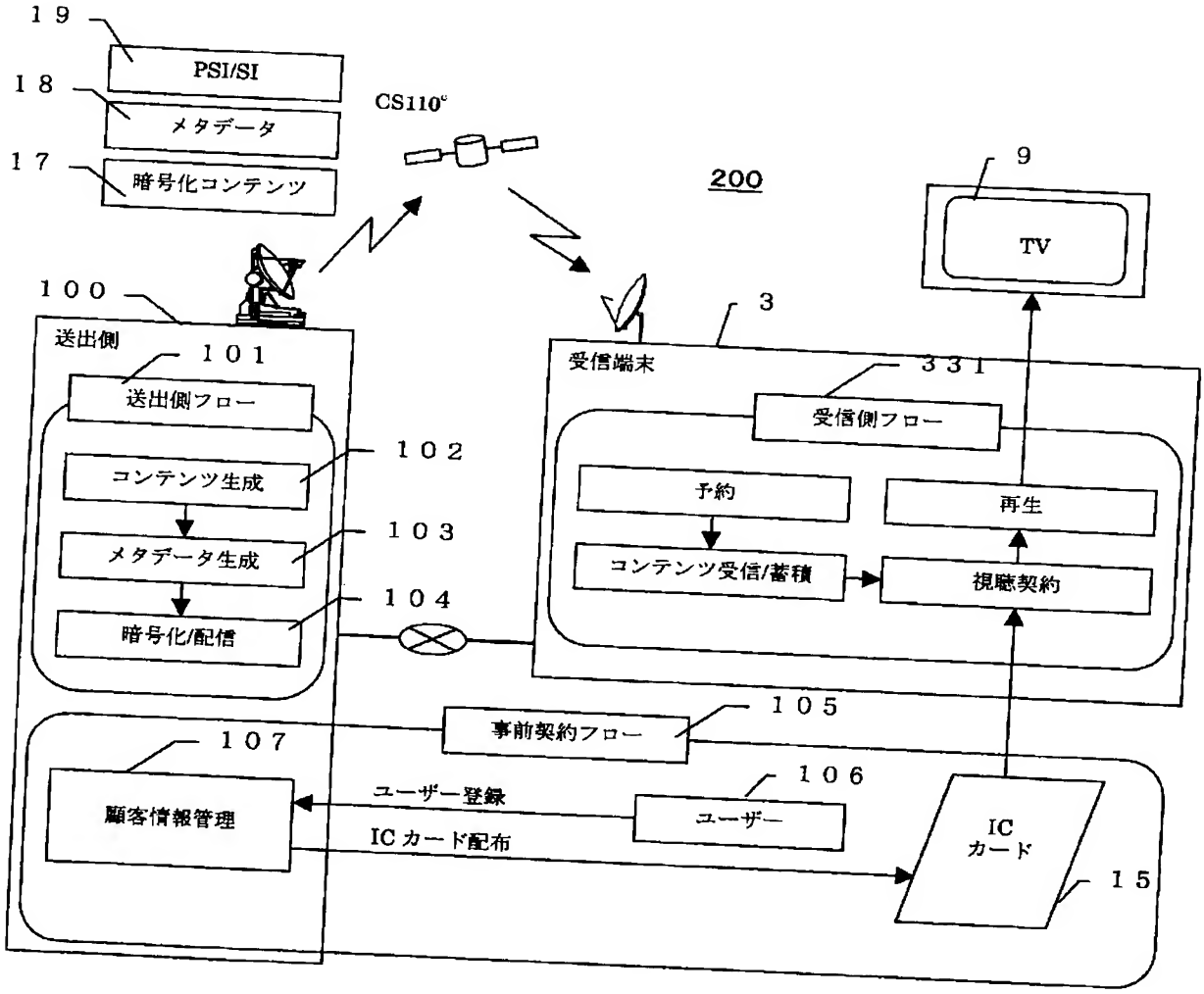
【図１０】


４０
事前契約用メタデータ
・端末ID
・個人ID
・オンラインPPV許諾
・etc
オンラインPPV許諾
４２
蓄積/再生用メタデータ
・コンテンツID
・視聴料金（５００円）
・etc
１００
コンテンツ
１９
送出側
顧客管理情報
課金情報
３
受信端末
１１
PPV登録（葉書 or 電話 or オンライン）
ユーザー
視聴分の料金
視聴料金要求
氏名
住所
年齢（生年月日）
電話番号
決済能力
決済先
契約事業者
契約形態
契約期間
要求ポイント数
etc
ユーザーID
端末ID
コンテンツID
料金
etc
５０
銀行/金融機関等
指定口座等
４８
５１

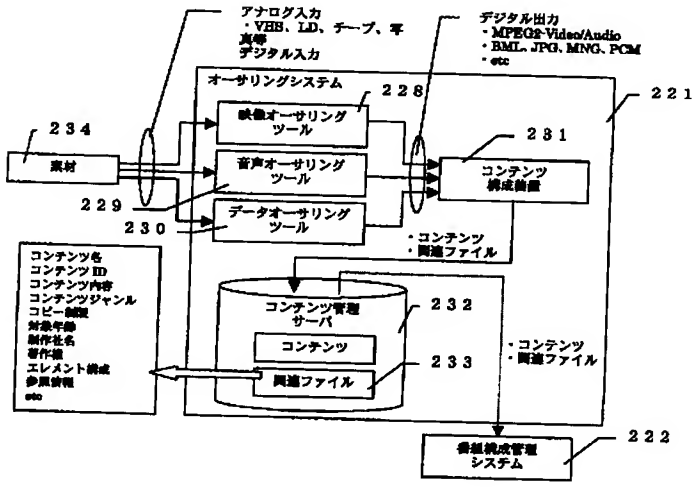
【図１６】


２２０
配信センタ
２２１
オーサリングシステム
２２４
PSI/SI生成装置
２２７
・PSI/SI
２２２
番組構成管理システム
・コンテンツ
・関連ファイル
・番組配列情報
２２５
コンテンツ暗号化装置
・暗号化コンテンツ
送出系システム
・コンテンツ
・関連ファイル
２２３
・配信位置（Locator）
メタデータ生成装置
・メタデータ
２２６
メタデータ暗号化装置
・暗号化メタデータ
２６０
顧客管理管理センタ
・メタデータ（事前契約用）
・鍵
・鍵
鍵管理センタ
２４０

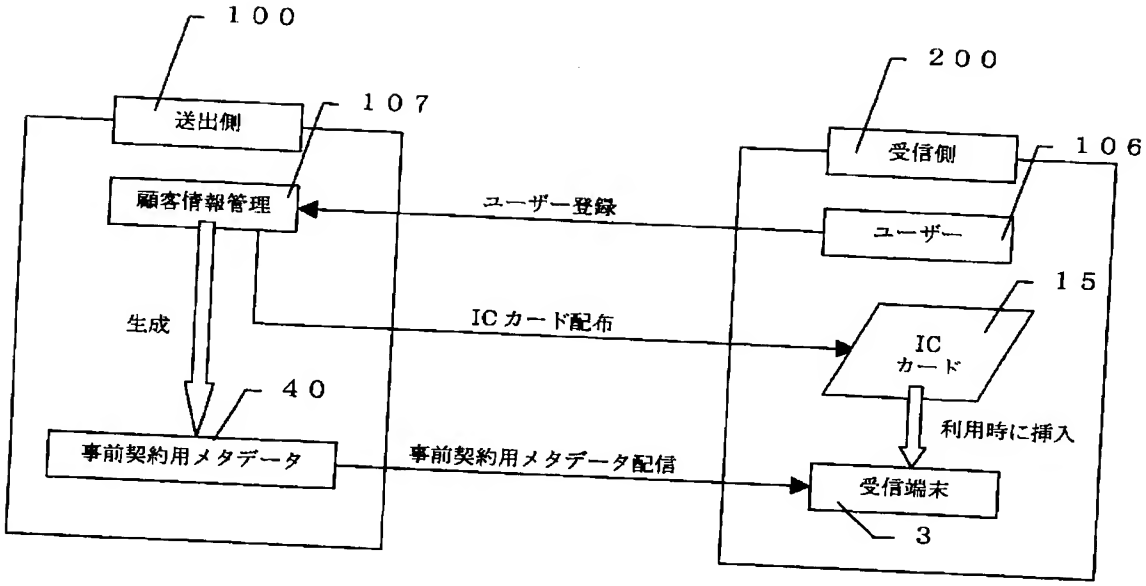
【図１１】


19
PSI/SI
18
メタデータ
17
暗号化コンテンツ
CS110°
200
9
TV
100
送出側
101
送出側フロー
102
コンテンツ生成
103
メタデータ生成
104
暗号化/配信
3
受信端末
331
受信側フロー
予約
再生
コンテンツ受信/蓄積
視聴契約
105
事前契約フロー
107
顧客情報管理
ユーザー登録
106
ユーザー
ICカード配布
ICカード
15

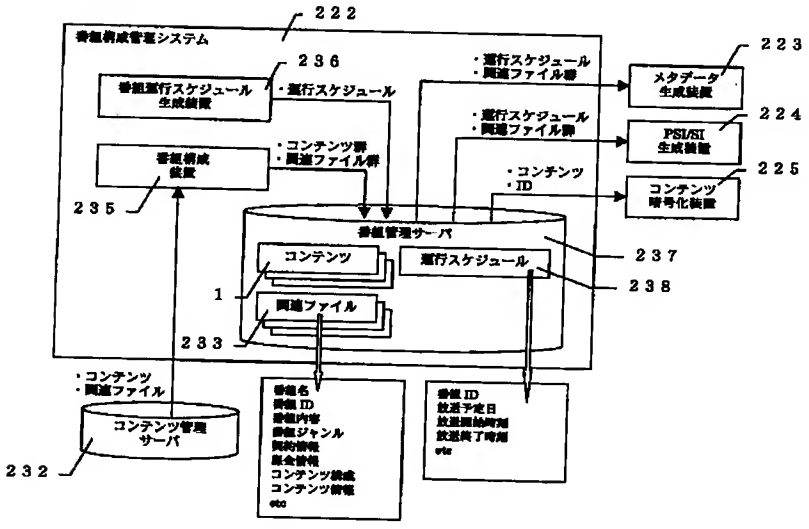
【図１７】


アナログ入力
・VHS、LD、テープ、等
高等
デジタル入力
デジタル出力
・MPEG2-Video/Audio
・BML、JPG、MNG、PCM
・etc
オーサリングシステム
228
221
234
素材
映像オーサリングツール
音声オーサリングツール
データオーサリングツール
229
230
231
コンテンツ構成管理
・コンテンツ
・関連ファイル
コンテンツ名
コンテンツID
コンテンツ内容
コンテンツジャンル
コピー制限
対象年齢
制作社名
著作権
エレメント構成
参照情報
etc
コンテンツ管理サーバ
232
コンテンツ
233
関連ファイル
・コンテンツ
・関連ファイル
番組構成管理システム
222

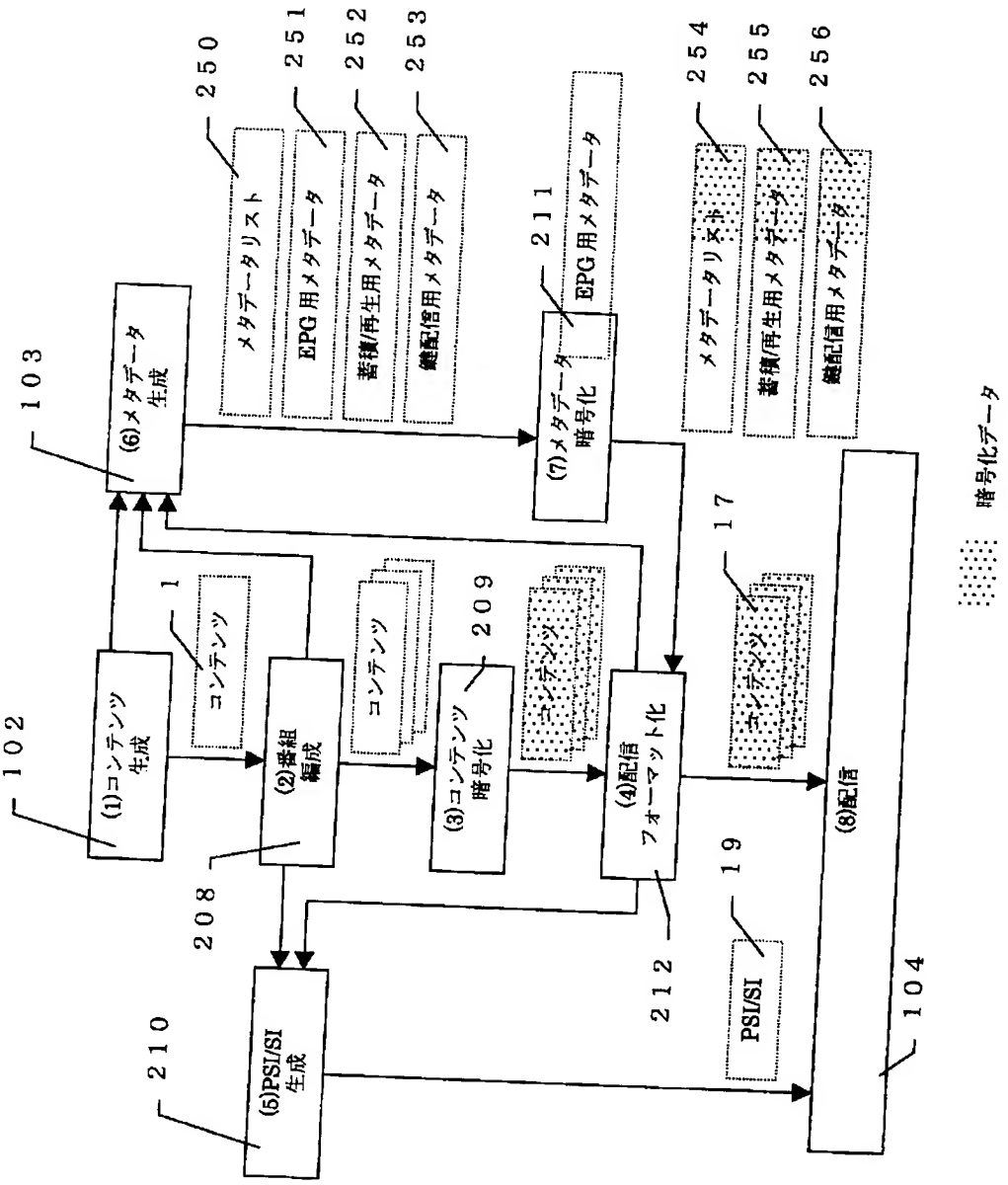
【図１２】


１００
送出側
１０７
顧客情報管理
生成
４０
事前契約用メタデータ
２００
受信側
１０６
ユーザー
ユーザー登録
１５
ICカード配布
IC
カード
利用時に挿入
事前契約用メタデータ配信
受信端末
３

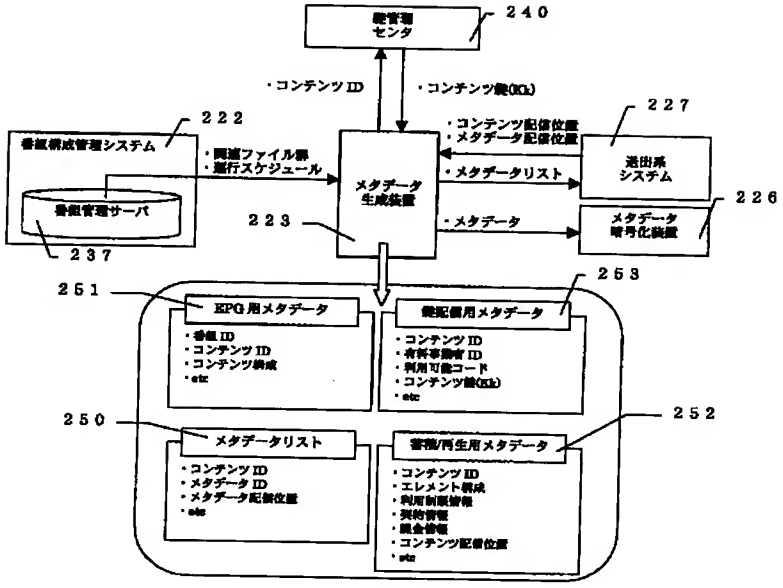
【図１８】


２２２
番組構成管理システム
２３６
番組運行スケジュール生成装置
・運行スケジュール
番組構成装置
・コンテンツ群
・関連ファイル群
２３５
・運行スケジュール
・関連ファイル群
メタデータ生成装置
２２３
PSI/SI生成装置
２２４
・コンテンツ
・ID
コンテンツ暗号化装置
２２５
番組管理サーバ
コンテンツ
運行スケジュール
２３７
２３８
1
関連ファイル
２３３
・コンテンツ
・関連ファイル
コンテンツ管理サーバ
２３２
番組名
番組ID
番組内容
番組ジャンル
放送予定日
放送開始時刻
放送終了時刻

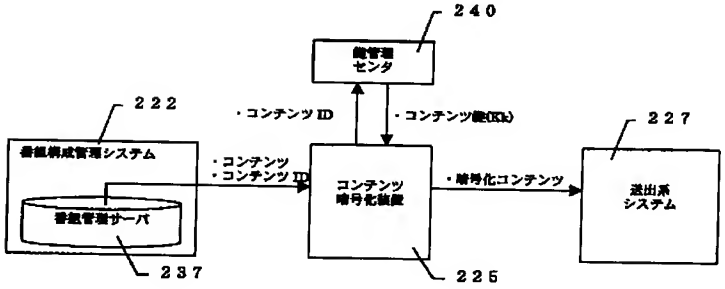
【図１３】


102
(1)コンテンツ生成
1
コンテンツ
(2)番組編成
208
209
コンテンツ
(3)コンテンツ暗号化
(4)配信フォーマット化
212
17
コンテンツ
19
PSI/SI
210
(5)PSI/SI生成
103
(6)メタデータ生成
250
メタデータリスト
251
EPG用メタデータ
252
蓄積/再生用メタデータ
253
継配信用メタデータ
211
(7)メタデータ暗号化
EPG用メタデータ
254
メタデータリスト
255
蓄積/再生用メタデータ
256
継配信用メタデータ
(8)配信
104
暗号化データ

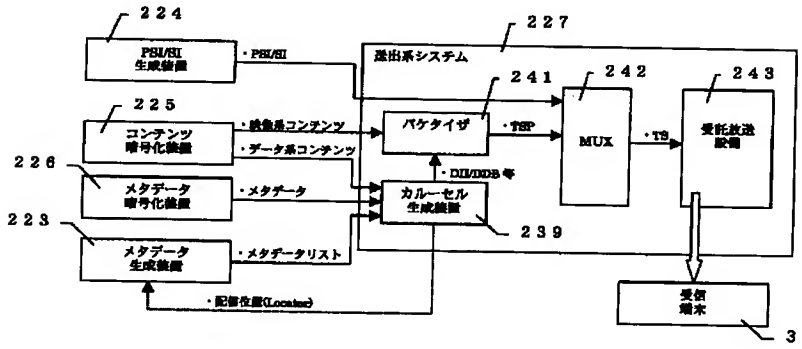
【図２０】


鍵管理センタ
240
・コンテンツID
・コンテンツ鍵(Kk)
222
番組構成管理システム
・関連ファイル群
・運行スケジュール
番組管理サーバ
237
メタデータ生成装置
223
・コンテンツ配信位置
・メタデータ配信位置
・メタデータリスト
・メタデータ
送出系システム
227
メタデータ暗号化装置
226
251
EPG用メタデータ
・番組ID
・コンテンツID
・コンテンツ構成
・etc
253
鍵配信用メタデータ
・コンテンツID
・有料等識者ID
・利用可能コード
・コンテンツ鍵(Kk)
・etc
250
メタデータリスト
・コンテンツID
・メタデータID
・メタデータ配信位置
・etc
252
番組/再生用メタデータ
・コンテンツID
・エレメント構成
・利用制限情報
・契約情報
・課金情報
・コンテンツ配信位置
・etc

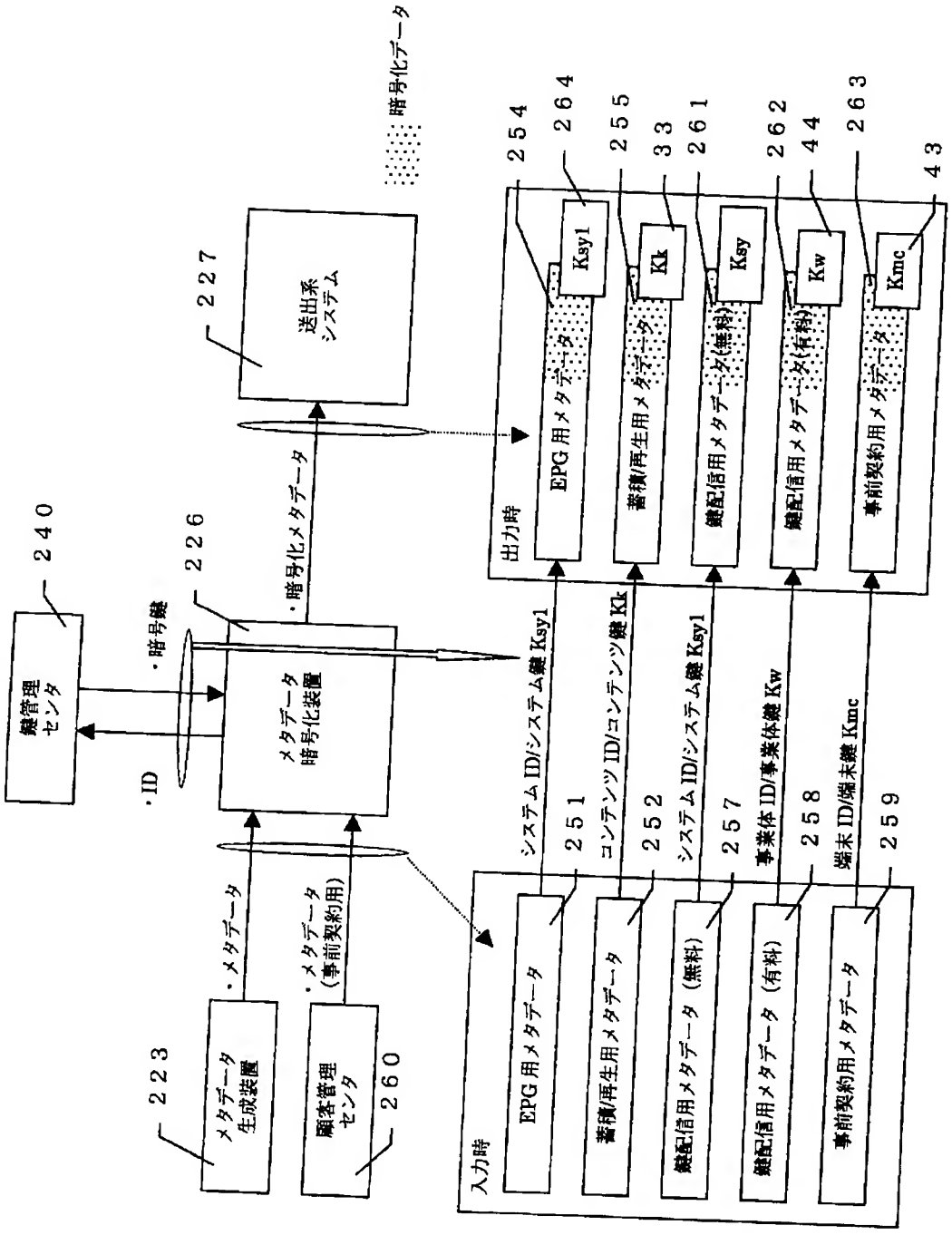
【図２１】


240
鍵管理センタ
222
番組構成管理システム
・コンテンツID
・コンテンツ鍵(Kk)
・コンテンツ
・コンテンツID
番組管理サーバ
237
コンテンツ暗号化装置
225
・暗号化コンテンツ
227
送出系システム

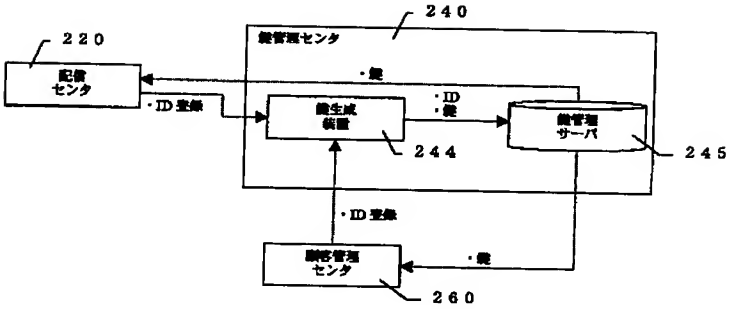
【図２３】


224
PSI/SI生成装置
・PSI/SI
227
送出系システム
241
242
243
225
コンテンツ暗号化装置
・映像系コンテンツ
・データ系コンテンツ
パケタイザ
・TSP
MUX
・TS
受託放送設備
226
メタデータ暗号化装置
・メタデータ
・DII/DDB等
223
メタデータ生成装置
・メタデータリスト
カルーセル生成装置
239
・配信位置(Locator)
受信端末
3

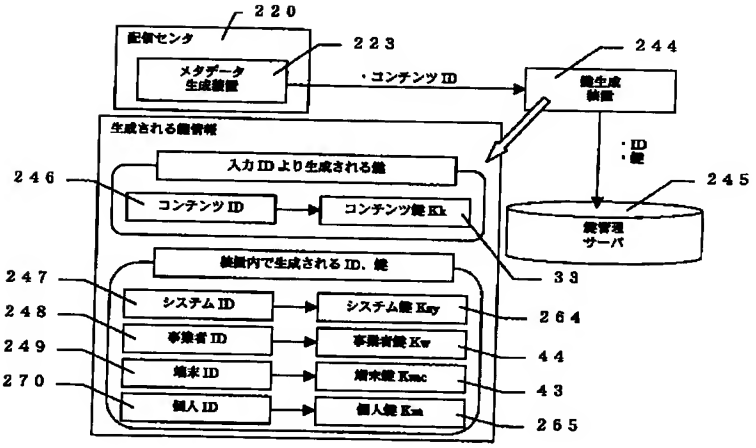
【図２２】


鍵管理センタ
240
・ID
・暗号鍵
メタデータ暗号化装置
226
・暗号化メタデータ
送出系システム
227
暗号化データ
メタデータ生成装置
223
・メタデータ
顧客管理センタ
260
・メタデータ(事前契約用)
入力時
EPG用メタデータ
蓄積/再生用メタデータ
鍵配信用メタデータ(無料)
鍵配信用メタデータ(有料)
事前契約用メタデータ
システムID/システム鍵 Ksy1
251
コンテンツID/コンテンツ鍵 Kk
252
システムID/システム鍵 Ksy1
257
事業体ID/事業体鍵 Kw
258
端末ID/端末鍵 Kmc
259
出力時
EPG用メタデータ
Ksy1
254
264
蓄積/再生用メタデータ
Kk
255
33
鍵配信用メタデータ(無料)
Ksy
261
262
鍵配信用メタデータ(有料)
Kw
44
事前契約用メタデータ
Kmc
263
43

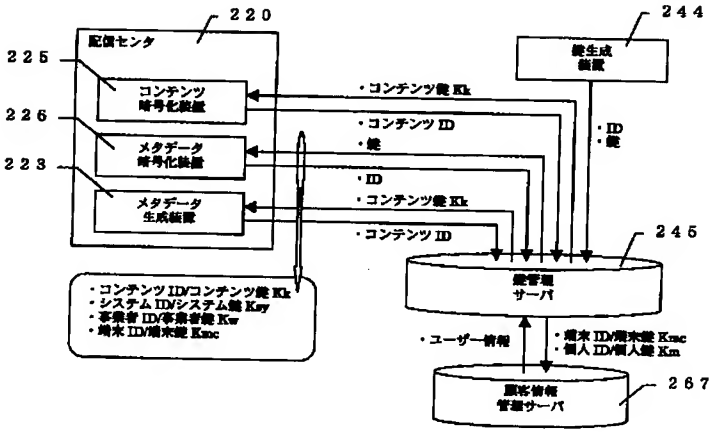
【図２４】


240
220
配信センタ
・鍵
・ID登録
・ID
・鍵
244
245
・ID登録
・鍵
260

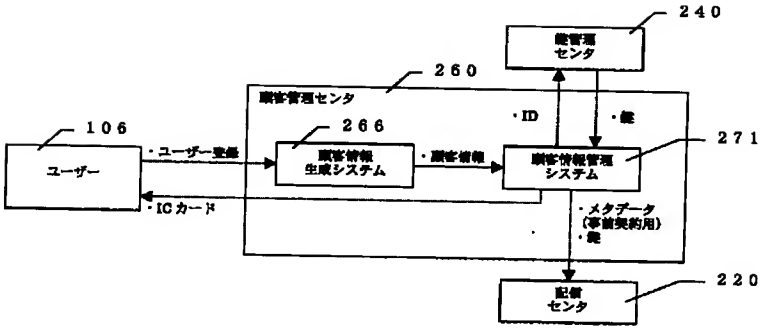
【図２５】


220
配信センタ
223
メタデータ生成装置
・コンテンツID
244
・ID
・鍵
245
246
入力IDより生成される鍵
コンテンツID
コンテンツ鍵Kk
33
247
248
249
270
システムID
事業者ID
端末ID
個人ID
システム鍵Kxy
事業者鍵Kw
端末鍵Kmc
個人鍵Km
264
44
43
265

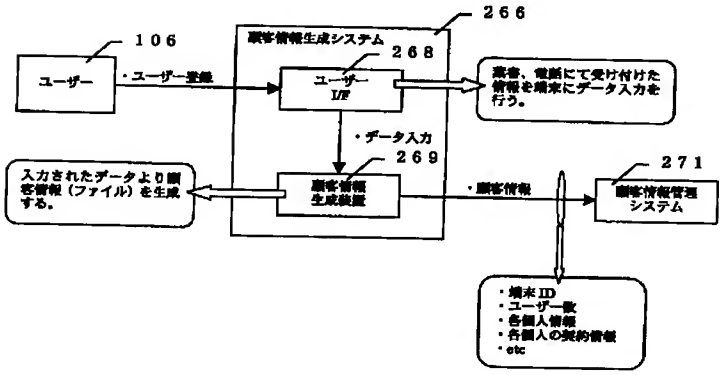
【図２６】


220
配信センタ
225
226
223
コンテンツ暗号化装置
メタデータ暗号化装置
メタデータ生成装置
・コンテンツ鍵Kk
・コンテンツID
・鍵
・ID
・コンテンツ鍵Kk
・コンテンツID
244
・ID
・鍵
245
・コンテンツID/コンテンツ鍵Kk
・システムID/システム鍵Kxy
・事業者ID/事業者鍵Kw
・端末ID/端末鍵Kmc
・ユーザー情報
・端末ID/端末鍵Kmc
・個人ID/個人鍵Km
267

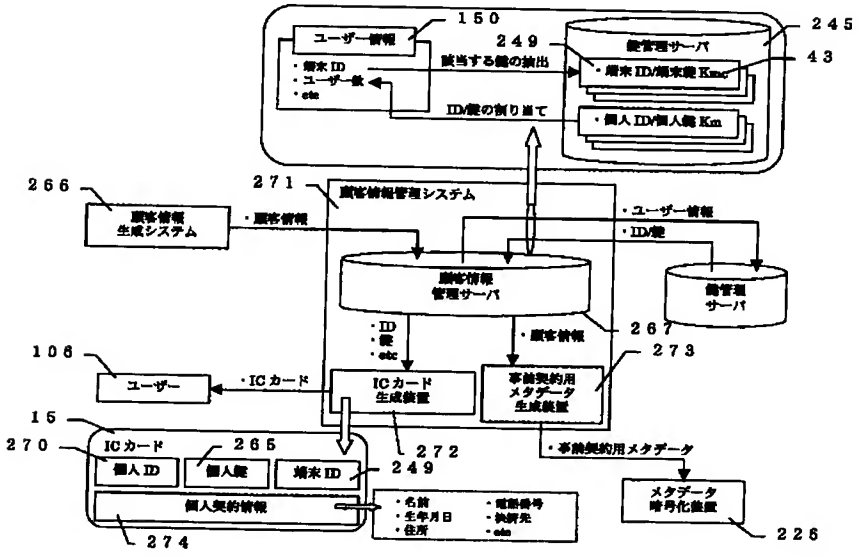
【図２７】


240
鍵管理センタ
260
顧客管理センタ
・ID
・鍵
106
ユーザー
・ユーザー登録
266
顧客情報生成システム
・顧客情報
271
顧客情報管理システム
・ICカード
・メタデータ（事前契約用）
・鍵
220
配信センタ

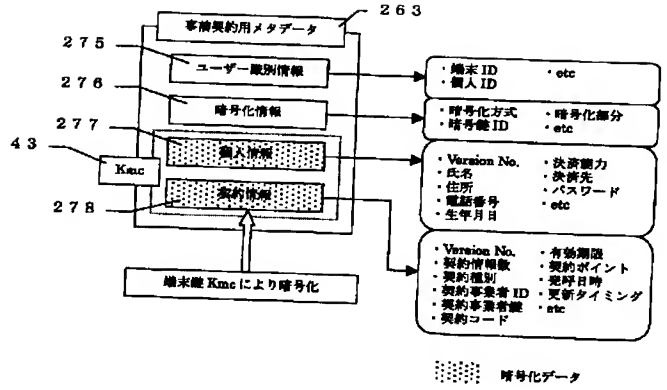
【図２８】


266
顧客情報生成システム
106
ユーザー
・ユーザー登録
268
ユーザーI/F
来客、電話にて受け付けた情報を端末にデータ入力を行う。
・データ入力
269
顧客情報生成装置
入力されたデータより顧客情報（ファイル）を生成する。
・顧客情報
271
顧客情報管理システム
・端末ID
・ユーザー数
・各個人情報
・各個人の契約情報
・etc

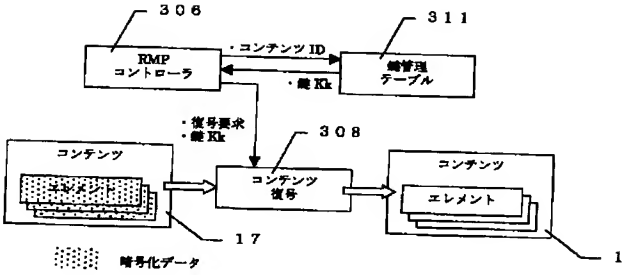
【図２９】


150
ユーザー情報
・端末ID
・ユーザー数
・etc
249
該当する鍵の抽出
ID/鍵の割り当て
245
鍵管理サーバ
43
・端末ID/端末鍵 Kmc
・個人ID/個人鍵 Km
266
顧客情報生成システム
・顧客情報
271
顧客情報管理システム
・ユーザー情報
・ID/鍵
顧客情報管理サーバ
鍵管理サーバ
267
・ID
・鍵
・etc
・顧客情報
106
ユーザー
・ICカード
ICカード生成装置
273
事前契約用メタデータ生成装置
15
270
ICカード
個人ID
265
個人鍵
端末ID
249
272
・事前契約用メタデータ
メタデータ暗号化装置
226
個人契約情報
・名前
・生年月日
・住所
・電話番号
・決済先
・etc
274

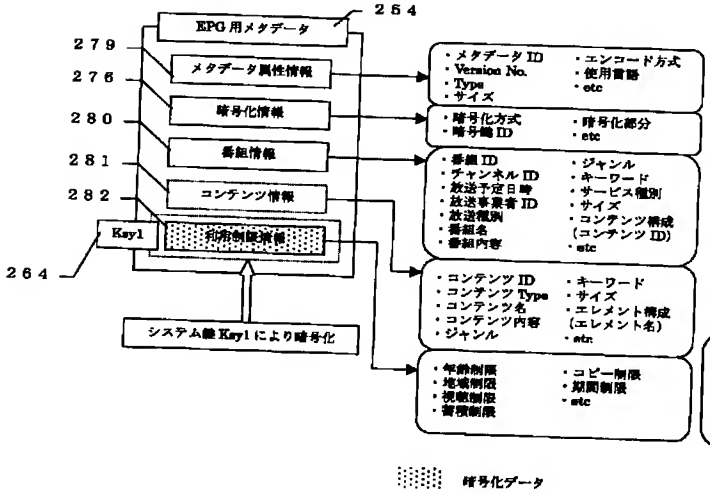
【図３０】



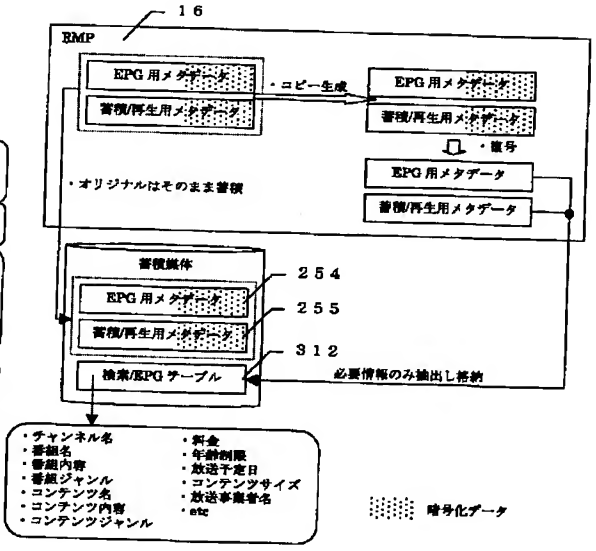
【図３８】



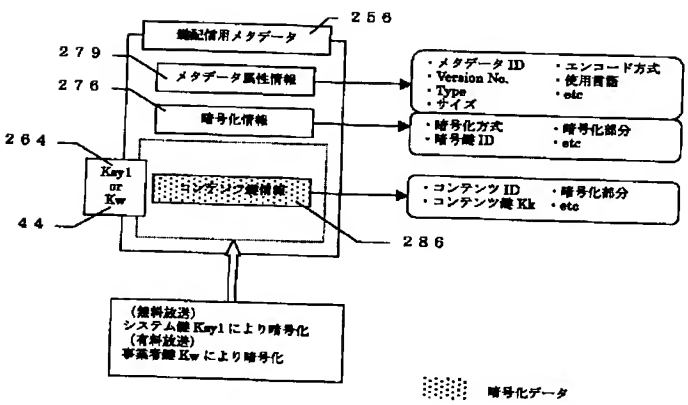
【図３１】



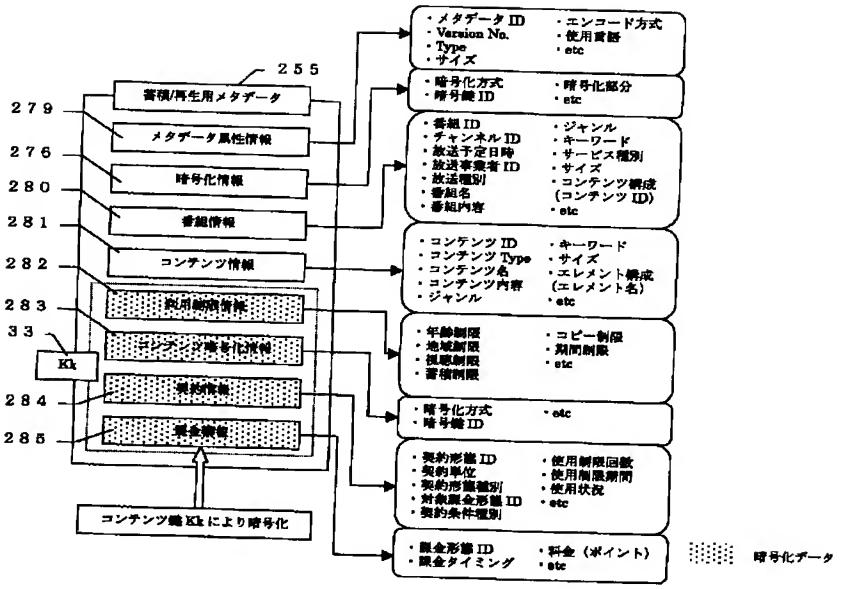
【図４６】



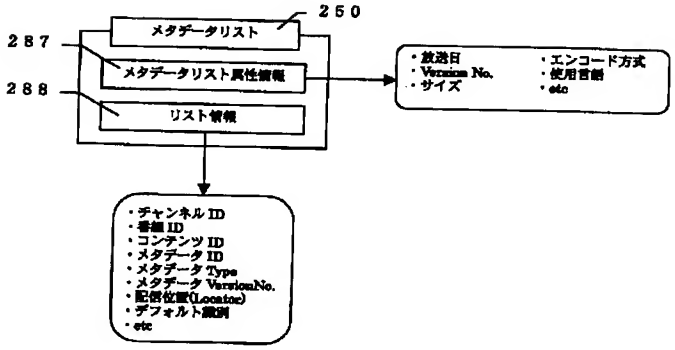
【図３３】



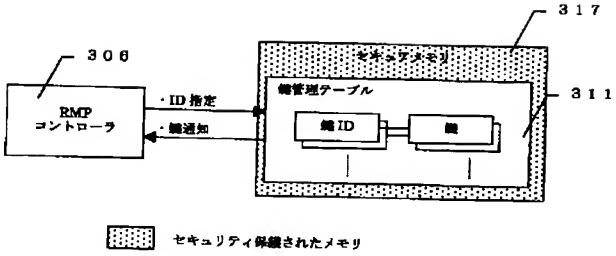
【図３２】



【図３４】



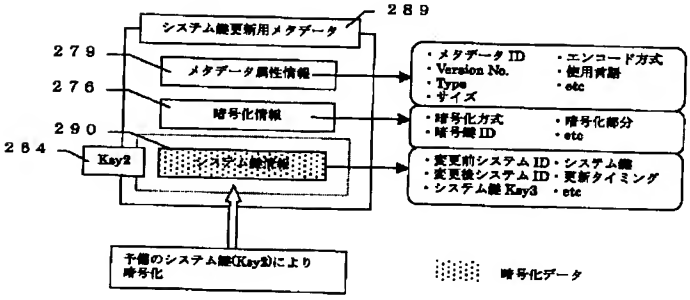
【図４０】



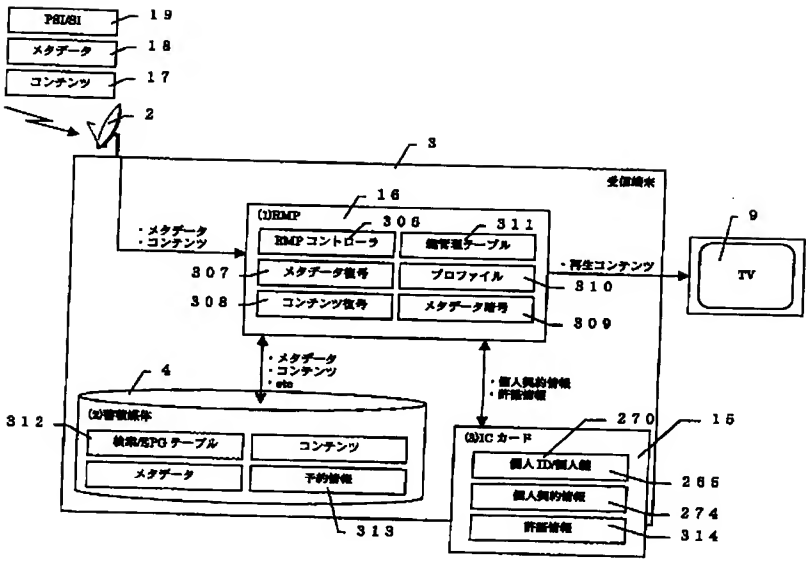
【図５０】

コンテンツ種別	エレメント
映像系コンテンツ	・MPEG2-Video stream(PES) ・MPEG2-Audio stream(PES) ・MPEG1-Video stream(PES) ・その他
データ系コンテンツ	・BML ・XML ・Text ・JPG ・GIF ・MPEG2-Video ・MPEG2-Audio ・MPEG1-Video ・MPEG1-PS ・MPEG2-PS ・その他

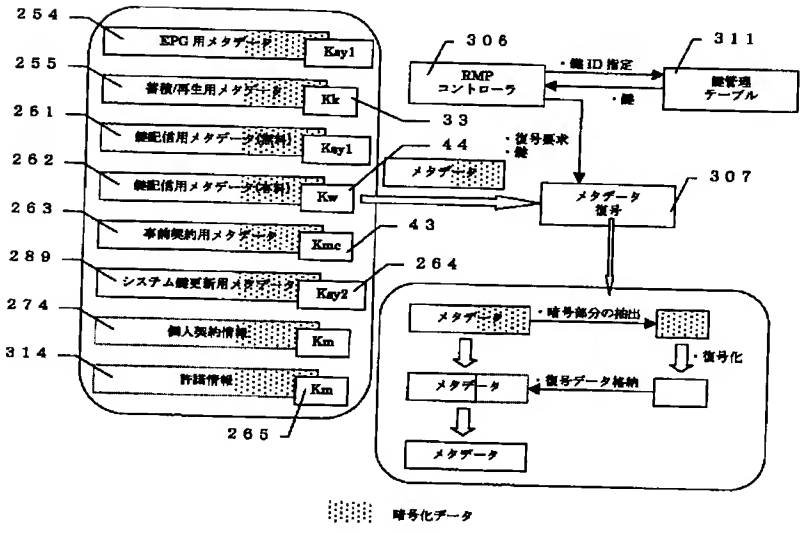
【図３５】



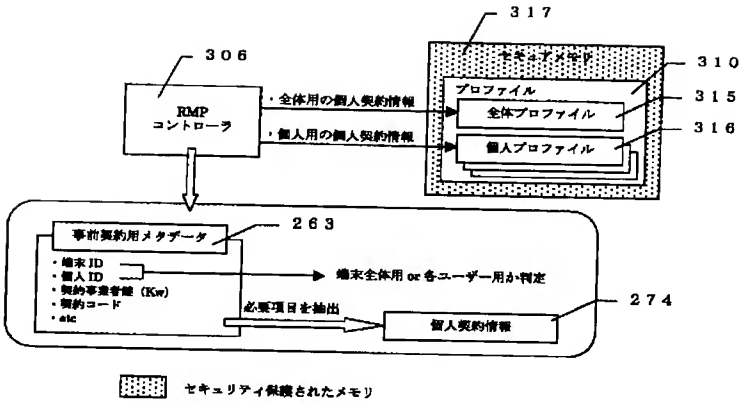
【図３６】


PSI/SI
19
メタデータ
18
コンテンツ
17
2
3
受信端末
16
(1)RMP
306
311
RMP コントローラ
鍵管理テーブル
307
メタデータ復号
プロファイル
310
308
コンテンツ復号
メタデータ暗号
309
・メタデータ
・コンテンツ
・再生コンテンツ
9
TV
・メタデータ
・コンテンツ
・etc
・個人契約情報
・許諾情報
4
(2)蓄積媒体
312
検索/EPG テーブル
コンテンツ
メタデータ
予約情報
313
(3)IC カード
270
15
個人 ID/個人鍵
265
個人契約情報
274
許諾情報
314

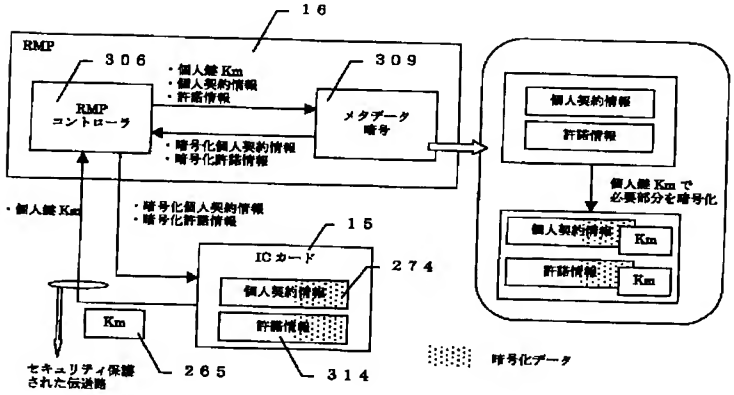
【図３７】


254
EPG 用メタデータ
Key1
255
蓄積/再生用メタデータ
Kk
33
261
録画/借用メタデータ(鍵)
Key1
262
録画/借用メタデータ(本体)
Kw
44
メタデータ
・復号要求
・鍵
263
事前契約用メタデータ
Kmc
43
289
システム鍵更新用メタデータ
Key2
264
274
個人契約情報
Km
314
許諾情報
Km
265
306
RMP コントローラ
・鍵 ID 指定
・鍵
311
鍵管理テーブル
307
メタデータ復号
メタデータ
・暗号部分の抽出
・復号化
メタデータ
・復号データ格納
メタデータ
暗号化データ

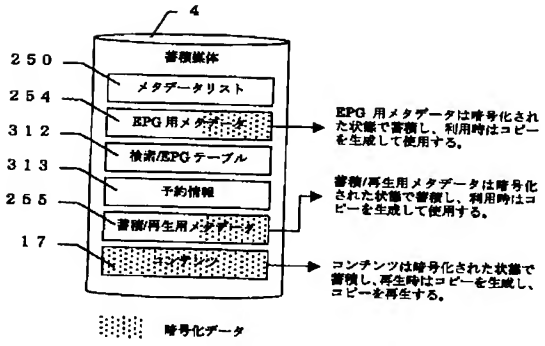
【図３９】


３１７
３０６
セキュアメモリ
３１０
RMP
コントローラ
・全体用の個人契約情報
・個人用の個人契約情報
プロファイル
３１５
全体プロファイル
３１６
個人プロファイル
事前契約用メタデータ
２６３
・端末ID
・個人ID
・契約事業者鍵（Kw）
・契約コード
・etc
端末全体用 or 各ユーザー用か判定
必要項目を抽出
２７４
個人契約情報
セキュリティ保護されたメモリ

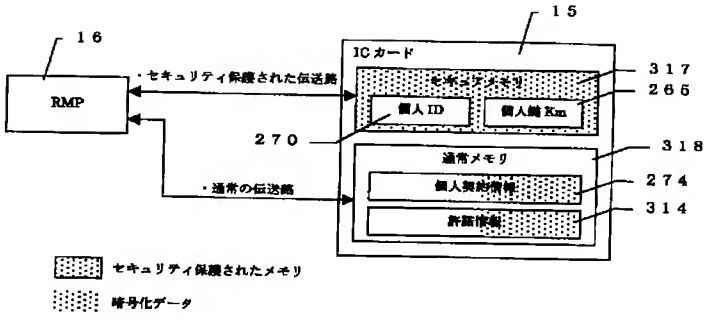
【図４１】


１６
RMP
３０６
RMP
コントローラ
・個人鍵 Km
・個人契約情報
・許諾情報
３０９
メタデータ
暗号
・暗号化個人契約情報
・暗号化許諾情報
個人契約情報
許諾情報
個人鍵 Km で
必要部分を暗号化
個人契約情報
Km
許諾情報
Km
・個人鍵 Km
・暗号化個人契約情報
・暗号化許諾情報
１５
ICカード
２７４
個人契約情報
許諾情報
Km
セキュリティ保護
された伝送路
２６５
３１４
暗号化データ

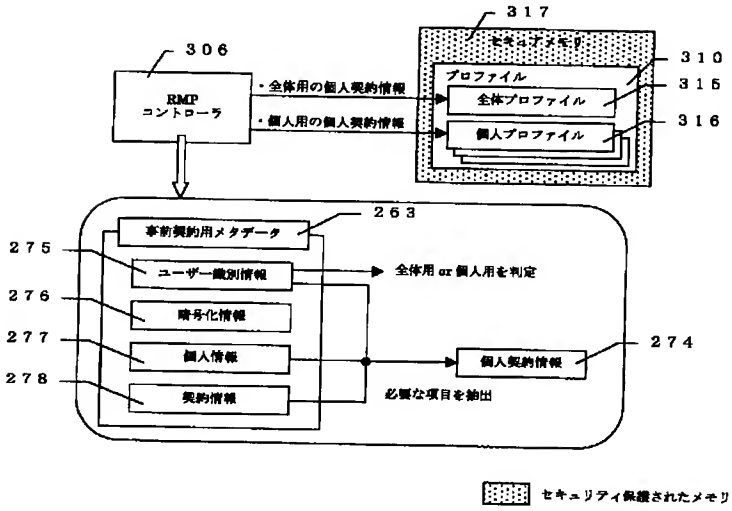
【図４２】


４
２５０
蓄積媒体
メタデータリスト
２５４
EPG 用メタデータ
３１２
検索/EPG テーブル
３１３
予約情報
２５５
蓄積/再生用メタデータ
１７
コンテンツ
EPG 用メタデータは暗号化された状態で蓄積し、利用時はコピーを生成して使用する。
蓄積/再生用メタデータは暗号化された状態で蓄積し、利用時はコピーを生成して使用する。
コンテンツは暗号化された状態で蓄積し、再生時はコピーを生成し、コピーを再生する。
暗号化データ

【図４３】



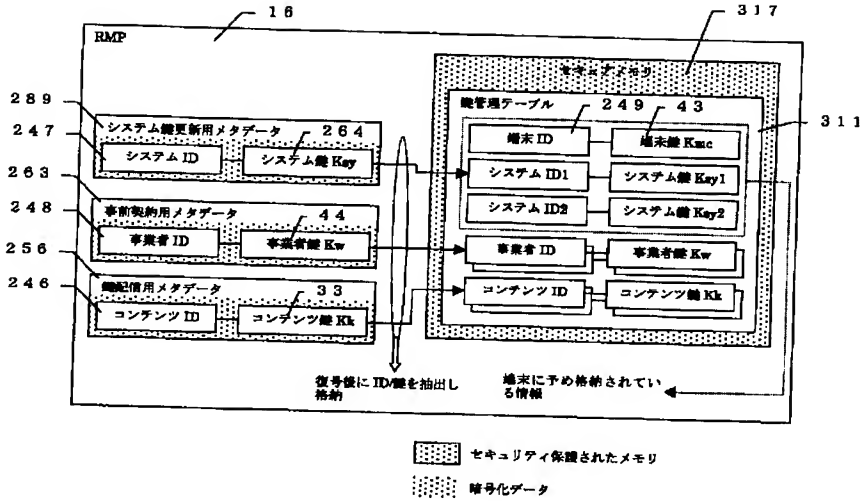
【図４４】



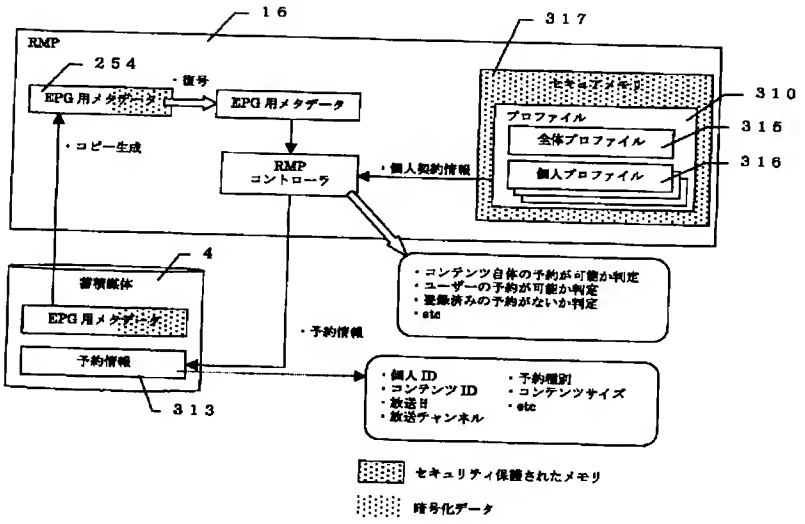
【図５１】

データ種別	暗号鍵種別	補足
コンテンツ	コンテンツ鍵（Kk）	コンテンツ毎に固有の鍵
メタデータリスト	無し	暗号化を行わない
事前契約用メタデータ	端末鍵（Knc）	端末毎に固有の鍵
EPG用メタデータ	システム鍵（Ksy1）	システム全体で共通の鍵
蓄積/再生用メタデータ	コンテンツ鍵（Kk）	コンテンツ毎に固有の鍵
鍵配信用メタデータ（無料）	システム鍵（Ksy1）	システム全体で共通の鍵
鍵配信用メタデータ（有料）	事業者鍵（Kv）	事業者毎に固有の鍵
システム鍵更新用メタデータ	システム鍵（Ksy2）	システム全体で共通の鍵（予備用）

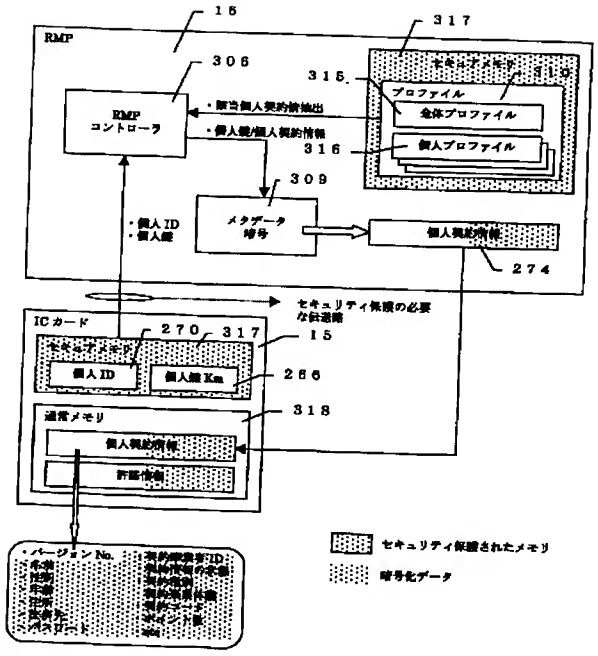
【図４５】


16
317
RMP
289
247
263
248
256
246
システム鍵更新用メタデータ
264
システム ID
システム鍵 Ksy
事前契約用メタデータ
44
事業者 ID
事業者鍵 Kw
録記信用メタデータ
33
コンテンツ ID
コンテンツ鍵 Kk
鍵管理テーブル
249
43
311
端末 ID
端末鍵 Kmc
システム ID1
システム鍵 Ksy1
システム ID2
システム鍵 Ksy2
事業者 ID
事業者鍵 Kw
コンテンツ ID
コンテンツ鍵 Kk
復号後に ID/鍵を抽出し格納
端末に予め格納されている情報
セキュリティ保護されたメモリ
暗号化データ

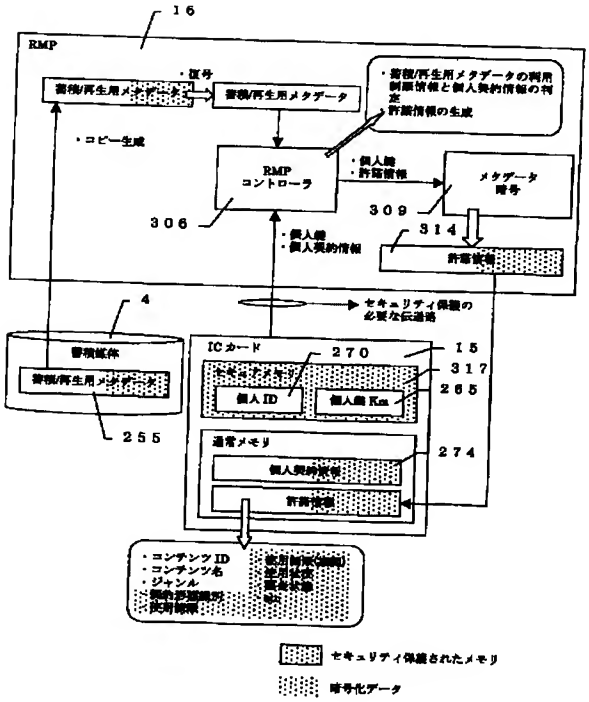
【図４７】


16
317
RMP
254
・復号
EPG 用メタデータ
EPG 用メタデータ
・コピー生成
RMP
コントローラ
・個人契約情報
プロファイル
全体プロファイル
個人プロファイル
310
316
316
4
蓄積媒体
EPG 用メタデータ
予約情報
313
・予約情報
・コンテンツ自体の予約が可能か判定
・ユーザーの予約が可能か判定
・登録済みの予約がないか判定
・etc
・個人 ID
・コンテンツ ID
・放送日
・放送チャンネル
・予約種別
・コンテンツサイズ
・etc
セキュリティ保護されたメモリ
暗号化データ

【図４８】



【図４９】



【図５２】

RMP コントローラの主な機能

機能	内容
受信制御	・蓄積/再生用メタデータ、録記信用メタデータ、プロファイルより受信可能なコンテンツかを判断し、コンテンツの受信を制御する機能
蓄積制御	・RMP 内部で発生するコンテンツ、メタデータ等の蓄積媒体への蓄積動作を EPG 用メタデータ、蓄積/再生用メタデータ、メタデータリスト等により制御する機能
コピー制御	・視聴契約等のユーザーリクエスト等により発生するリムーバブルメディア等へのコピー要求を蓄積/再生用メタデータの情報により制御する機能
提示制御	・ユーザーの視聴要求に対し蓄積/再生用メタデータの情報、視聴契約により生成された許諾情報をもとにコンテンツの再生を制御する機能
視聴契約制御	・蓄積/再生用メタデータ、IC カード内の個人契約情報をもとにコンテンツの視聴に対する許諾情報を生成する機能
課金制御	・蓄積/再生用メタデータに格納されたポイント情報等と、IC カード内の個人契約情報をもと行われる課金処理を制御する機能
個人認証制御	・各メタデータ内にユーザーを制限する情報がある場合に、プロファイル、IC カード内の個人契約情報をもとに行われる認証処理を制御する機能
鍵管理	・受信端末内の鍵を管理する機能
プロファイル管理	・事前契約用メタデータから生成される各個人、端末のプロファイルを管理する機能
時刻管理	・受信端末における時刻情報を管理する機能
アプリケーション認証制御	・Plug In アプリケーション等に対する認証を制御する機能
外部機器認証制御	・受信端末に接続される外部機器に対する認証を制御する機能
通信回線制御	・視聴履歴、課金情報等の権利保護が必要な情報を通信回線を利用し送出側に送信する際に通信路の安全性に関する制御を行う機能

フロントページの続き

(51) Int. Cl.[7]		識別記号
H04N	5/76	
	5/91	
	7/167	
	7/173	640

FI			テーマコード(参考)
H04N	7/173	640A	
H04L	9/00	601B	
H04N	7/167	Z	
	5/91	P	

(72)発明者 山崎 伊織
東京都千代田区神田駿河台四丁目6番地
株式会社日立製作所放送・通信システム推進事業部内

Fターム(参考) 5C052 AB02 CC01 DD04 DD06
5C053 FA20 FA28 GB05 JA21 LA11 LA15
5C064 BB01 BB02 BC04 BC17 BC22 BC23 BC25 BD08 BD09
5J104 EA10 EA17 NA02 PA05 PA11

【公開番号】特開２００２－２１７８９４
【公報種別】特許法第１７条の２の規定による補正の掲載
【ＳＴ公報種別】A5
【公開日】２００２年（２００２）８月２日
【出願番号】特願２００１－２９５７２２
【発行日】２００７年（２００７）１月２５日
【部門区分】第７部門第３区分
【国際特許分類第８版】
H04L 9/08 F
G06F 13/00 U
G06Q 30/00 U
G06Q 50/00 U
H04N 5/76 U
H04N 7/173 U
H04N 7/167 U
H04N 5/91 U
【ＦＩ】
H04L 9/00 601 B
G06F 13/00 520 B
G06F 17/60 302 E
G06F 17/60 332
G06F 17/60 ZEC
H04N 5/76 Z
H04N 7/173 640 A
H04N 7/167 Z
H04N 5/91 P

【手続補正書】
【提出日】２００６年（２００６）１１月３０日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】

【特許請求の範囲】
【請求項１】
コンテンツおよび該コンテンツに対して付与され、該コンテンツの再生に利用されるメタデータを受信側へ送信するコンテンツ送信装置において、
上記コンテンツに関連する情報を含み、該情報の用途に応じて複数のメタデータを生成するメタデータ生成手段と、
上記複数のメタデータを上記コンテンツを受信する側へ送信するメタデータ送信手段と
を備え、
コンテンツの再生に利用されるメタデータを複数生成し、受信側へ送信することを特徴とするデータ送信装置。
【請求項２】
上記コンテンツに関連する情報が、ユーザと事業者間の契約に関するコンテンツ利用契約情報、コンテンツ暗号化鍵情報、コンテンツの利用を判定するための利用制限情報、コンテンツの視聴／蓄積予約を行う情報のうちのいずれかひとつ又は複数であり、
上記複数のメタデータが、上記利用契約情報を含む事前契約用メタデータ、上記コンテンツ暗号化鍵情報を含む鍵配信用メタデータ、上記利用制限情報を含む蓄積／再生用メタ

データ、コンテンツ視聴／蓄積予約情報を含むEPG用メタデータのうちのいずれか複数である請求項１記載のデータ送信装置。

【請求項３】

更に、上記複数のメタデータのコンテンツ関連情報に基づいて上記メタデータの情報を識別するためのメタデータリストを生成する手段を備えた請求項１記載のデータ送信装置。

【請求項４】

更にシステム鍵更新用メタデータを生成する手段を備えた請求項１記載のデータ送信装置。

【請求項５】

コンテンツおよび該コンテンツの蓄積、再生に利用されるメタデータを送信する方法において、

ユーザ側からの契約要求に基づきコンテンツの利用契約情報を含む事前契約用メタデータを生成するステップと、

ユーザ側からのコンテンツ要求にもとづきコンテンツを再生するコンテンツ鍵を含む鍵配信用メタデータおよびコンテンツの利用制限情報を含む蓄積／再生用メタデータを生成するステップと、

上記事前契約用メタデータおよび上記蓄積／再生用メタデータの保護を必要とする部分に暗号化を施す暗号化ステップと、

上記暗号化部を含むメタデータをユーザ側に送信するステップと、

ユーザ側からのコンテンツ受信要求に基づきコンテンツを上記コンテンツ鍵にて暗号化してユーザ側に送信するステップと、

を含むコンテンツ送信方法。

【請求項６】

コンテンツおよび該コンテンツに対して付与され、該コンテンツに関連する情報に応じた複数のメタデータを受信するコンテンツ受信装置であって、

コンテンツ鍵により暗号化されたコンテンツおよび保護が必要な部分を暗号化したコンテンツ利用契約情報を含む契約用メタデータ、コンテンツ鍵を含む鍵配信用メタデータ、コンテンツの蓄積／再生用メタデータを受信する受信手段と、

上記受信コンテンツおよび上記複数のメタデータを蓄積する蓄積手段と、

上記複数のメタデータの暗号を解除し復号するメタデータ復号手段と、

上記メタデータに基づき蓄積手段のコンテンツを読み出し、該読み出しコンテンツを上記コンテンツ鍵により復号するコンテンツ復号手段と、

上記コンテンツ復号手段により復号されたコンテンツを表示する表示手段と、

上記コンテンツ復号手段および上記メタデータ復号手段により復号されたコンテンツおよびメタデータを暗号化し、上記蓄積手段に蓄積する手段と

を備えたコンテンツ受信装置。

【請求項７】

コンテンツおよび該コンテンツに対して付与され、該コンテンツの再生に利用されるメタデータを送受信するコンテンツ送受信システムにおいて、

上記コンテンツに関連する情報を含み、該情報に応じた複数のメタデータを生成するメタデータ生成手段と、

上記複数のメタデータを上記コンテンツを受信する側へ送信するメタデータ送信手段と、

上記コンテンツおよび上記複数のメタデータを受信する受信手段と、

上記受信コンテンツおよび上記複数のメタデータを蓄積する蓄積手段と、

上記複数のメタデータの暗号を解除し復号するメタデータ復号手段と、

上記メタデータに基づき蓄積手段のコンテンツを読み出し、該読出しコンテンツに上記コンテンツ鍵により復号するコンテンツ復号手段と、

上記コンテンツ復号手段により復号されたコンテンツを表示する表示手段と、

上記コンテンツ復号手段および上記メタデータ復号手段により復号されたコンテンツおよびメタデータを暗号化し、上記蓄積手段に蓄積する手段と、
を備えたコンテンツ送受信システム。【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００４
【補正方法】変更
【補正の内容】

【０００４】
【発明が解決しようとする課題】
配信コンテンツ等のデータ改ざん、不正利用等が防止可能なコンテンツ送信サービスシステム、方法、装置を提供することにある。【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】削除
【補正の内容】

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】

【０００７】
【課題を解決するための手段】
本発明は、コンテンツに対して付与され、該コンテンツの再生に利用されるメタデータをコンテンツ関連情報の用途に応じて複数のメタデータを生成し、コンテンツ受信側に送信する構成とした。【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】削除
【補正の内容】

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正の内容】

【０００９】
また、本発明は、コンテンツを構成するエレメントと上記メタデータとを蓄積する蓄積手段と、上記暗号化コンテンツを復号する第１の復号手段と、上記メタデータの暗号化されたデータを復号する第２の復号手段と、上記第１の復号手段にて復号された再生コンテンツを外部メディアに供給する手段と、上記第１、第２の復号手段にて復号されたデータ又は装置内で生成されるデータを暗号化する手段（３０９）とを設けた構成とした。【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００８３
【補正方法】変更
【補正の内容】

【００８３】
【発明の効果】

本発明によれば、コンテンツの再生に利用されるメタデータをコンテンツ関連情報の用途に応じて複数生成して送信することにより、受信側でのコンテンツの不正利用等をより確実に防止することが可能である。